D3.3 - Mechanisms and Tools for Regulatory Compliance I

Title	D3.3 - Mechanisms and Tools for Regulatory Compliance I
Revision Number	1.0
Task reference	T3.5
Lead Beneficiary	NUIG
Responsible	Bardia Khorsand, Martin Serrano
Partners	AL, BPFI, IQB, KM, UNP
Deliverable Type	DEM
Dissemination Level	PU
Due Date	2024-03-31 [Month 15]
Delivered Date	2024-08-02
Internal Reviewers	GFT
Quality Assurance	UPRC
Acceptance	Coordinator Accepted
Project Title	FAME - Federated decentralized trusted dAta Marketplace for Embedded finance
Grant Agreement No.	101092639
EC Project Officer	Stefano Bertolo
Programme	HORIZON-CL4-2022-DATA-01-04

This project has received funding from the European Union's Horizon research and innovation programme under Grant Agreement no 101092639

Revision History

Version	Date	Partners	Description
0.1	2024-03-28	NUIG	TOC
0.6	2024-05-14	NUIG, AL, BPFI, IQB, KM, UNP	Contents updates
0.7	2024-05-17	NUIG, AL, BPFI, IQB, KM, UNP	Contents updates
0.8	2024-06-04	NUIG, AL, BPFI, IQB, KM, UNP	Contents updates
1.0	2024-08-02	NUIG	Version for submission

Definitions

Acronyms	Definition
4AML	4th Anti Money Laundering Directive
4AMLD	4th Anti Money Laundering Directive
AI	Artificial Intelligence
BPFI	Banking and Payments Federation Ireland
CD	Continuous Development
DGA	Data Governance Act
DPA	Data Protection Authority
DPO	Data Protection Officer
DSP	Digital Service Providers
EBA	European Banking Authority
EC	European Commission
ESG	Environmental, Social and Governance
EU	European Union
FAME	Federated decentralized trusted dAta Marketplace for Embedded finance
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
HW	HardWare
ICT	Information Communication Technologies
ID	Identity
IDS	International Data Spaces
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
KM	KM Cube Anonymi Etaireia Parochis Ependytikon Ypiresion
NIS	Network and Information Systems
NUIG	National University Of Ireland Galway
OES	Operators of Essential Services
PSD	Payment Services Directive
PSD2	2nd Payment Services Directive
PSDII	Second Payment Service Directive
PSP	Payment Service Provider

PSR	Project Security Responsible
RTS	Regulatory Technical Standard
SA	Supervisory Authority
SCA	Strong Customer Authentication
SW	SoftWare
TFEU	Treaty on the Functioning of the European Union
UNP	Unparallel Innovation

Executive Summary

Recently, some of the most advanced marketplaces have been developed in Europe which provides functionalities for data catalogues, search, analytics, trading, and accounting. Marketplaces such as i3-MARKET, DataVaults, MOSAICrOWN, MUSKETEER provide value-added features for integrating, accessing, and trading data assets, such as data assets monetization, data sovereignty, personal data protection, compliance to regulations (e.g., to GDPR (General Data Protection Regulation)). FAME's ambition is to deliver Europe's first standards-based, secure, regulatory compliant, interoperable, and federated data marketplace platform for Embedded Finance (EmFi) applications. Apart from unique feature of the FAME project, which is federated access control, the project provides a unified access to all related regulations in the field. In that sense, it provides a harmonious ecosystem of the laws and regulations according to the need of different stakeholders.

Regulatory compliance tools based on the definition and enforcement of policies that ensure compliance with applicable laws and regulations such as GDPR, the PSD2 (2nd Payment Services Directive), and the 4AML (4th AntiMoney Laundering directive. The main objective of the regulatory compliance tool is to ensure compliance of the FAME project functionalities with related laws and regulations that is to comply with the security and regulatory requirements of EmFi applications. In so doing, regulatory compliance tools is set according to the prominent regulations of the sector (i.e., PSD2, MiFIDII, 4AML) in addition to general regulations (e.g., GDPR AI Act). Therefore, the ultimate regulatory compliance asset is a tool applicable for unified data policies management in-line with security-by-design and regulatory compliance by design principles.

This Deliverable reports the background study of the related laws and regulations as well as the prototype implementations of the FAME regulatory compliance tool. We also ensure all key achievements and milestones are highlighted to showcase the progress and impact of the project succinctly. The following aspects of the related laws and regulations are highlighted and demonstrated as part of the objective(s) for the regulatory compliance tool reported in this document:

- The possibility of the mapping between FAME and related projects in the field.
- The laws and regulations framework of the similar projects.
- The background study on the related laws and regulations.
- The prototype of the regulatory compliance tool website

Table of Contents

List of Figures

1 Introduction

FAME is a joint effort of world class experts in data management, data technologies, the data economy and digital finance to develop, deploy and launch to the global market a unique, open, publicly accessible, trustworthy, energy efficient, and secure federated data marketplace for EmFi, which will offer novel decentralized programmable pricing and trading of data assets. The FAME data marketplace will alleviate the proclaimed limitations of centralized cloud marketplaces towards demonstrating the full potential of the data economy. In this direction, the project will enhance a state of the art data marketplace infrastructure (namely the H2020 i3-MARKET marketplace) with novel functionalities in three complementary directions namely: (i) Secure, interoperable and regulatory compliant data exchange across multiple federated cloud-based data providers in-line with emerging.

The regulatory landscape of the finance sector has been traditionally very dynamic and volatile. Significant changes in regulations and/or the emergence of new regulations could therefore lead to changes in the FAME marketplace implementation. This could delay the realization of the project's impacts. However, by providing a thorough review of the related laws and regulations we aim to mitigate the adverse impact of dynamic laws and regulation on the project.

We take a systemic approach in reviewing the related laws and regulations. We divide the potential stakeholders into financial institutions, non-financial institutions, public entities, platforms, and individuals. Then we identify three categories of laws and regulations, namely regulations, policy, and standard and guidelines. The related laws and regulations then study in whole by providing detail of each law and regulations. We further provide some information on the mapping between FAME and other related projects name GAIA-X and IDSA.

FAME offers regulatory compliance tools that will ease compliance to applicable regulations. It will also provide support for reliable data provenance, which will ease support for new regulatory rules. In this document we provide an overview of the desined website for regulatory compliance tool. This website summarizes regulatory ecosystem of the Europe in a user friendly way. The users would be able to browse through related laws and regulation and gain access to information regarding regulatory framework. We also suggest an access control for laws and regulation according to the field of their applications.

WP3 is devoted to the implementation of the project's secure, regulatory compliant access to the various federated marketplace, which will lead to the production of the federated catalogue of data assets. Moreover, WP3 will specify the FAME ontologies and will implement the semantic interoperability framework. The WP3 models and ontologies will be used to support the implementation of trusted and efficient analytics in WP5 and the use cases in WP6.

T3.5 Regulatory Compliance Tools (M5-M27; Leader: NUIG; Part.: IQB, KM, UNP, BPFI, AL): This task will specify and implement security policies and data policies that will boost the compliance of data assets to applicable regulations in EmFi UCs (focus on NUIG, IQB). To this end, the security policy management tools of the project will be used to produce various regulatory support and regulatory compliance tools. The work will be driven by the regulatory requirements that will be specified in WP2 and will provide support for regulations like PSDII (focus on BPFI), GDPR (focus of AL), MiFiD (focus of KM), the EU taxonomy for ESG investments (focus of KM), as well as the emerging EU AI Act (focus of AL). In conjunction with the ethical and legal management task of WP1, this task will also specify how the various tools will be used to support the regulation of the FAME marketplace in-line with applicable laws and directives.

This document describes the specifications and the implementation of the regulatory compliance tool for FAME, providing regulatory landscape of the project. D3.3 Mechanisms and Tools for Regulatory Compliance: Prototypes of the regulatory compliance tools (T3.5).

1.1 Objective of the Deliverable

The objective of this deliverable is to document regulatory compliance tool and to present a prototype of the website relating to related laws and regulations.

The FAME regulatory compliance tool objective is to provide a user-centric tool or wizard that present related laws and regulations in a user-friendly environment. To do so, we propose a regulatory framework that relates to all associated laws and regulations.

1.2 Insights from other Tasks and Deliverables

The purpose of this deliverable is to document the outcomes of Task 3.5 Regulatory Compliance Tools. This deliverable aims to present the FAME regulatory compliance tool. This task will specify and implement security policies and data policies that will boost the compliance of data assets to applicable regulations in EmFi UCs (focus on NUIG, IQB). To this end, the security policy management tools of the project will be used to produce various regulatory support and regulatory compliance tools. The work will be driven by the regulatory requirements that will be specified in WP2 and will provide support for regulations like PSDII (focus on BPFI), GDPR (focus of AL), MiFiD (focus of KM), the EU taxonomy for ESG investments (focus of KM), as well as the emerging EU AI Act (focus of AL). In conjunction with the ethical and legal management task of WP1, this task will also specify how the various tools will be used to support the regulation of the FAME marketplace in-line with applicable laws and directives.

As such, this deliverable receives input and refers to work developed as fully open source in other tasks in FAME project and IDSA project. This deliverable primarily serves as first specification and implementation prototype report and as main input for the subsequent deliverables of FAME Work Package 3 (WP3).

1.3 Structure

The deliverable is structured as follows:

Chapter 1 Introduction:

This section serves as the gateway to the deliverable, detailing the main objectives and goals of the document within the context of the FAME project.

Chapter 2 Positioning of FAME in the context of similar projects:

In this section, the deliverable is contextualized within the larger framework of the FAME laws and regulations.

Chapter 3 Background study on related laws and regulations:

This crucial section delves into the specifics of laws and regulations within the FAME project. It includes a comprehensive examination of the related laws and regulations. In this sense, each law is study thoroughly by providing details of each regulation.

Chapter 4 Prototype of the website relating to laws and regulations:

This section is dedicated to demonstrating the practical application of the key components discussed in previous section. It includes detailed information on the prototype website.

Chapter 5 Conclusions:

The final section of the deliverable encapsulates the key findings, insights, and outcomes derived from the analysis and demonstrations of the FAME SA and its components. It provides a summary of the deliverable, touching on the significant achievements and the Key Performance Indicators (KPIs) met, as outlined in the document.

2 Positioning of FAME in the context of European Initiatives:

2.1 FAME versus GAIA-X and IDSA

Figure 1 presents FAME regulatory framework. We divided the potential stakeholders in five groups, namely financial institutions, non-financial institutions, public entities, platforms, and individuals. We also define three main areas in which FAME is located. That is regulations, policy, and standards and guidelines.

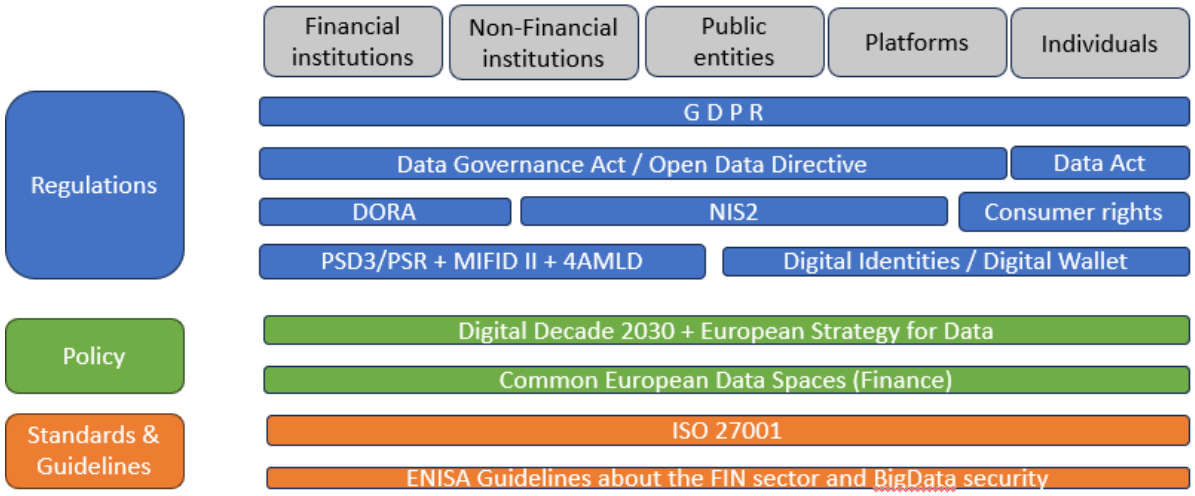


Figure 1 FAME Regulatory Framework

Figure 2 illustrates the FAME regulatory triangle. Accountability, responsibility, and liability are one side of the triangle where transparency, trust, engagement, and success by design is another side of the triangle. Contracts, regulations and legislations, standardisation and guidelines and ethics are the main components of the regulatory triangle.

Figure 2 FAME regulatory triangle!

While GAIAX provides no specific resolution on the regulatory requirement objectives the IDSA background study on laws and regulation is more comprehensive. The IDSA project complies with GDPR and major regulations in Europe, however they do not provide comprehensive analysis on the related laws and regulations unlike FAME project task 3.5.

IDSA provides a short description of the user-based format while in FAME, we provide a comprehensive study of the related laws and regulations in the systematic manner. For example, we divide the potential users into groups based on their nature and provide related laws and regulations accordingly. We base our analysis on Europe in the same way as what IDSA offers.

Given all these points, we are positive that mapping between IDSA and FAME is possible.

2.2 Background study on GAIA-X

Gaia-X is an initiative that develops, based on European values, a digital governance that can be applied to any existing cloud/ edge technology stack to obtain transparency, controllability, portability and interoperability across data and services. Gaia-X is not a market operator, nor will it operate directly or exclusively any of the services required by the governance.

It enables a federated and secure data infrastructure, whereby data are shared, with users retaining control over their data access and usage. It enables the creation of links between many cloud service providers in a wider, transparent and fair ecosystem to drive the European Data economy of tomorrow.

Gaia-X aims to create a federated open data infrastructure based on European values regarding data and cloud sovereignty. The mission of Gaia-X is to design and implement a data sharing architecture that consists of common standards for data sharing, best practices, tools, and governance mechanisms. It also constitutes an EU-anchored federation of cloud infrastructure and data services, to which all 27 EU member states have committed themselves1. This overall mission drives the Gaia-X Architecture.

Gaia-X is:

- A non-profit association in which its members define the Gaia-X architecture & rules
- Gaia-X makes and supports others to make open-source implementations of its specifications
- A qualification authority for the Gaia-X Label, including the Basic Conformity
- GAIA-X project provides no specific resolution on the regulatory requirement objectives.

Gaia-X is Not:

- A formal standardisation body
- A SW or HW product or cloud platform
- A runtime implementation of any Gaia-X service

Data Spaces: What are they?

The term ‘data space’ refers to a type of data relationship between trusted partners who adhere to the same high level standards and guidelines in relation to data storage and sharing within one or many Vertical Ecosystems.A critical aspect of the data space notion is that data are not stored centrally, but rather at the source. Thus, they are only transferred through semantic interoperability as necessary.

A data space is the sum of all its participants, which may be data providers, users and intermediaries. Data spaces can be nested and overlapping. For instance, a data provider can participate in several data spaces all at once. Each Data Space provides specific data. Thereby, it forms a solid ground for one or many ecosystems. The software required to implement data spaces runs on cloud/edge cloud infrastructures.

Data spaces objectives and deliverables within Gaia-X

The main objective of Gaia-X is to create the conditions for an outburst of data within the European market. Key to this is the creation of data spaces, which are the digital representation of existing physical or natural or industrial or social ecosystems. In a data space, several actors belonging to the same value chain (all suppliers and oem in a supply chain, all public and private transportation in a smart city, all hospitals and laboratories in a healthcare, and so forth) federate each other to exchange data. Given the data space create services and insights that can only be achieved through the federation of the multiple actors, every single actor earns a value in participating to the federation that it could not achieve using its data only.

Gaia-X aims to develop data space projects to create an economy of data in several domains, from private to public sector. Through data space projects, Gaia-X will be developed in the market and Gaia-X services will be made available through marketplaces restricted to the federation participants or open to the outside of the federation.

The Gaia-X Association enables the creation of data spaces through the work of the regional hubs. Each hub has the objective to focus on its regional strategic data spaces, and develop concrete business cases creating consortia of member companies around them.

Gaia-X enabled data spaces allow for:

- scaling individual solutions to address new customers
- extending existing solutions with new value propositions
- combine existing solutions to enable collaborations in ecosystems.

Data spaces can be industry-specific or cross-industries, they can involve multiple player within a territory or across territories, and provide for the only way to reduce physical barriers, reduce time to market, leverage the distributed intelligence and create additional value for all, large and small players, users and providers of technology.

Through data space creation, Europe can leverage the most accessible and highest quality raw material that can reinforce our economy by winning the battle of competitivity in the digital era: high quality data. From automotive to healthcare, agriculture to education, transportation, energy or finance, the European processes, legislation, and industrial ecosystem feature by far the highest complexity and quality, and therefore are the way to win the battle to competitivity in the creation of high quality digital products and services.

According to our research, GAIA-X does not provide an stand-alone regulatory compliance framework.

2.3 Background study on the International Data Spaces Association

The International Data Spaces Association (IDSA) is on a mission to create the future of the global, digital economy with International Data Spaces (IDS), a secure, sovereign system of data sharing in which all participants can realize the full value of their data.

As an association we are subject to the provisions of the Federal Data Protection Act (BDSG) and the Telemedia Act (TMG). We have taken technical and organisational measures to ensure that the data protection regulations are observed both by us and by external service providers.

Personal data is information that can be used to determine a user's identity. This includes information such as username, address, postal address and telephone number. Information that is not directly associated with the real identity of the user (such as favourite websites or number of users of a site) is not included. Users can use our online offering without disclosing their identity. Personal data is only collected if the user provides it of his or her own accord – for example when registering, making an enquiry via the contact page or submitting an online application.

Access to this data is only possible for a few specially authorised persons who are involved with the technical or editorial support of the servers. In connection with user access, data are stored on our servers for security purposes which may allow identification (for example IP address, date, time and pages viewed). These data are not utilized in a personalised form. We reserve the right to statistically evaluate anonymised data records.

The IP address is stored for data security reasons in order to guarantee the stability and operational security of our system.

1 Name and Address of the controller

Controller for the purposes of the General Data Protection Regulation (GDPR), other data protection laws applicable in Member states of the European Union and other provisions related to data protection is:

International Data Spaces e. V.

Emil-Figge-Str. 80

44227 Dortmund, Germany

Phone: +49 (0) 231 70096 – 501

info@internationaldataspaces.org

Website: www.internationaldataspaces.org

2 Disclosure of personal information to third parties

We do not pass on personal information to third parties without the users' explicit consent. Should data be passed on to service providers within the scope of order data processing, they are bound by the BDSG and other legal regulations. In so far as we are legally obliged to or obliged to do so by court order, we will transfer your data to such bodies that are legally entitled to receive such information.

3 Right of withdrawal

Personal user data can be deleted at any time on request. We set "cookies" (small files with configuration information) in the majority of the internet pages we maintain according to the specifications of the Informationgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e. V. – IVW (German Audit Bureau of Circulation) and for measuring access to advertising media. They

help to determine the frequency of use and the number of users of our websites. We do not collect any personal data via cookies. In some areas of our website we use cookies to implement user functions. Our website can also be used without cookies. Most browsers are set to accept cookies automatically. However, the user can deactivate the storage of cookies or set his or her browser in a way that he or she is informed as soon as cookies are sent.

4 Children

Persons under the age of 18 should not transmit any personal data to us without the consent of their parents or legal guardians.

5 Links

Our website may contain links to other websites. We have no influence over whether their operators comply with the data protection regulations.

6 Reserve the right to change

The rapid development of the internet requires adjustments to the data protection declaration from time to time. We will inform you of any necessary changes.

7 Cookies

Our Internet pages use cookies. Cookies are text files that are stored in a computer system via an Internet browser.

Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the dats subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

Through the use of cookies, the IDSA can provide the users of this website with more user-friendly services that would not be possible without the cookie setting.

By means of a cookie, the information and offers on our website can be optimized with the user in mind. Cookies allow us, as previously mentioned, to recognize our website users. The purpose of this recognition is to make it easier for users to utilize our website. The website user that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user’s computer system. Another example is the cookie of a shopping cart in an online shop. The online store remembers the articles that a customer has placed in the virtual shopping cart via a cookie.

The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

8 Subscription to our newsletters

On our website, users are given the opportunity to subscribe to our enterprise's newsletter. The input mask used for this purpose determines what personal data are transmitted, as well as when the newsletter is ordered from the controller.

The IDSA informs its customers and business partners regularly by means of a newsletter about enterprise offers. The enterprise's newsletter may only be received by the data subject if (1) the data subject has a valid e-mail address and (2) the data subject registers for the newsletter shipping. A confirmation e-mail will be sent to the e-mail address registered by a data subject for the first time for newsletter shipping, for legal reasons, in the double opt-in procedure. This confirmation e-mail is used to prove whether the owner of the e-mail address as the data subject is authorized to receive the newsletter.

During the registration for the newsletter, we also store the IP address of the computer system assigned by the Internet service provider (ISP) and used by the data subject at the time of the registration, as well as the date and time of the registration. The collection of this data is necessary in order to understand the (possible) misuse of the e-mail address of a data subject at a later date, and it therefore serves the aim of the legal protection of the controller.

The personal data collected as part of a registration for the newsletter will only be used to send our newsletter. In addition, subscribers to the newsletter may be informed by e-mail, as long as this is necessary for the operation of the newsletter service or a registration in question, as this could be the case in the event of modifications to the newsletter offer, or in the event of a change in technical circumstances. There will be no transfer of personal data collected by the newsletter service to third parties. The subscription to our newsletter may be terminated by the data subject at any time. The consent to the storage of personal data, which the data subject has given for shipping the newsletter, may be revoked at any time. For the purpose of revocation of consent, a corresponding link is found in each newsletter. It is also possible to unsubscribe from the newsletter at any time directly on the website of the controller, or to communicate this to the controller in a different way.

9 Newsletter-Tracking

The newsletter of the IDSA contains so-called tracking pixels. A tracking pixel is a miniature graphic embedded in such e-mails, which are sent in HTML format to enable log file recording and analysis. This allows a statistical analysis of the success or failure of online marketing campaigns. Based on the embedded tracking pixel, the IDSA may see if and when an e-mail was opened by a data subject, and which links in the e-mail were called up by data subjects.

Such personal data collected in the tracking pixels contained in the newsletters are stored and analyzed by the controller in order to optimize the shipping of the newsletter, as well as to adapt the content of future newsletters even better to the interests of the data subject. These personal data will not be passed on to third parties. Data subjects are at any time entitled to revoke the respective separate declaration of consent issued by means of the double-opt-in procedure. After a revocation, these personal data will be deleted by the controller. The IDSA automatically regards a withdrawal from the receipt of the newsletter as a revocation.

10 Contact possibility via the website

The website of the IDSA contains information that enables a quick electronic contact to our enterprise, as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address). If a data subject contacts the controller by e-mail or via a contact form, the personal data transmitted by the data subject are automatically stored. Such personal

data transmitted on a voluntary basis by a data subject to the data controller are stored for the purpose of processing or contacting the data subject. There is no transfer of this personal data to third parties.

11 Routine erasure and blocking of personal data

The data controller shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the European legislator or other legislators in laws or regulations to which the controller is subject to.

If the storage purpose is not applicable, or if a storage period prescribed by the European legislator or another competent legislator expires, the personal data are routinely blocked or erased in accordance with legal requirements.

12 Legal basis for the processing

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR. Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

13 Rights of the data subject

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact any employee of the controller.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information.

Furthermore, the European directives and regulations grant the data subject access to the following information:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;

the existence of the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact any employee of the controller.

c) Right to rectification

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact any employee of the controller.

d) Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.

The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.

The personal data have been unlawfully processed.

The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by the IDSA, he or she may, at any time, contact any employee of the controller. An employee of IDSA shall promptly ensure that the erasure request is complied with immediately.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. An employees of the IDSA will arrange the necessary measures in individual cases.

e) Right of restriction of processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.

The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by the IDSA, he or she may at any time contact any employee of the controller. The employee of the IDSA will arrange the restriction of the processing.

f) Right to data portability

Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and

machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact any employee of the IDSA.

g) Right to object

Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

The IDSA shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

If the IDSA processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to the IDSA to the processing for direct marketing purposes, the IDSA will no longer process the personal data for these purposes.

In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by the IDSA for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact any employee of the IDSA. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Automated individual decision-making, including profiling

Each data subject shall have the right granted by the European legislator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision (1) is not is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, or (3) is not based on the data subject’s explicit consent.

If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject's explicit consent, the IDSA shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any employee of the IDSA.

i) Right to withdraw data protection consent

Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact any employee of the IDSA.

14 Web Analytics/Tracking

Our website uses the Matomo open source software by InnoCraft Ltd in New Zealand to analyze the activities of our website users and to optimize our website and its content based on this analysis. In so doing we do not obtain any information that identifies you directly.

The Matomo version we use takes precautions based on DoNotTrack technology (see on this www.donottrack.us) to ensure your website search is not captured if you have set your internet browser to stop tracking.

The use of Matomo involves cookies and tracking pixels which allow statistical analysis of the use of this website based on your visits. The cookie saves information, including personal information, on your visiting behavior on our website, which Matomo then processes under a pseudonym in a user profile for analytical purposes. . Since we host Matomo on our own servers, the analysis does not require data processing by third parties.

Without your specific permission, we neither use the data collected to identify you personally nor will we match the data with personal data pertaining to the pseudonym associated with you.

If IP addresses are collected, they are immediately anonymized after collection by deleting the last number block.

We process statistical data based on our legitimate interest pursuant to Article 6 (1) lit. f GDPR to optimize our online offering and our web presence.

New EU regulatory environment for data spaces

The EU Commission published the "European Strategy for Data" in 2020 to create a single market for data that ensures Europe's global competitiveness and data sovereignty.

As part of this strategy, the Commission proposed different regulations:

- AI Act Proposal (AIA-E)

- Data Act Proposal (DA-E)
- Data Governance Act (DGA)
- Digital Markets Act (DMA)
- Digital Services Act (DSA)

The complexity of the regulatory framework is increasing, but the regulations are not yet aligned, and the interplay with existing legislation such as data protection laws, competition laws, or regulations on intellectual property is not clear. Also, the terminology is not aligned, which causes difficulties in their interpretation and interoperability with existing legislation.

The new regulations differ regarding their subject matter and scope. While the DMA and the DSA are instruments to regulate competition and rights in the digital market, the DA-E and the DGA mainly concern access and use of data. The AI Act can be seen as a separate proposal with little connection to the others. With respect to B2B data spaces, the more general DA-E and DGA will have the greatest impact, while the other regulations are less central in this scope.

Considerations regarding DA-E and DGA

The DA-E concerns the rights to access and use data generated by Internet of Things (IoT) devices. Therefore, it applies to roles related to such data, including manufacturers, data holders, data recipients, and providers of data processing services. As the DA-E covers the whole lifecycle of data processing, it may impact use cases in the data space as the data needs to be handled in compliance (e.g., the grant of access rights).

Due to its broad definitions, the DA-E leaves considerable room for interpretation, creating legal uncertainty. Another uncertainty concerns the interfering with existing contracts and the DA-E impact on the contractual freedom. The freedom to negotiate should be restricted as little as possible to encourage the building of value chains and innovation. Imbalances could instead be addressed through EU competition law or sector-specific legislation. It remains to be seen to what extent the DA-E will undergo adjustments to create legal certainty and practical solutions for data sharing.

The DGA comes also with some concerns, especially regarding the broad definitions for the roles in data sharing (e.g., data holder, data user). Also, how it addresses services provider roles does not cover the complexity of data spaces. The envisioned data governance and the respective roles do not achieve the intended goals of facilitating data sharing. Given the complex roles and services within data spaces, the DGA term “data intermediation services” needs to be aligned with practice as data spaces use different terms for data sharing services.

The DGA defines a number of obligations (such as notification and compliance requirements), especially regarding intermediation service providers, that play a key role in the data economy:

- Obligation for data sharing service providers to notify competent authority.
- Conditions for providing data sharing services, such as neutrality, fair, transparent, and non-discriminatory access to services, adequate technical, legal, and organizational measures to prevent transfer or access to non-personal data that is unlawful under Union law.

The European Commission decided to adopt this approach to ensure that data governance within the Union is based on trustworthy sharing of data. A key element in increasing trust and control of data

holders, data subjects, and data users is the neutrality of data intermediation service providers concerning the data shared. It is necessary for these providers to act only as intermediaries and not use the data shared for any other purpose.

The approach and key elements of IDS concepts reflect the DGA's goal of trustworthy data sharing, which involves neutral intermediaries and reliance on reference architecture, connector technology, and certifications.

Challenges and opportunities for EU's DIB in developing common data spaces

The DGA approach comes with several challenges. It only frames general rules, while the details are subject to national laws and need to be translated into practical solutions. The European Data Innovation Board (EDIB), proposed by the DGA, will play a fundamental role. It will support the EU Commission in issuing guidelines to facilitate the development of common European data spaces, as well as identifying standards and interoperability requirements for cross-sector data sharing.

There might be a link between the DGA and other regulations on the topic of interoperability standards. For example, the DA-E defines that the guidelines for "interoperability specifications for the functioning of common European data spaces, such as architectural models and technical standards implementing legal rules and arrangements between parties that foster data sharing, such as regarding rights to access and technical translation of consent or permission" should come from the EU Commission. Therefore, it is likely that such guidelines will come from the EDIB under the DGA. It will be beneficial to link these tasks to achieve harmonized rules in practice between both regulations.

This task will directly relate to the activities of data space initiatives such as IDSA, which will play a major role, as they have already developed frameworks and reference architectures that can act as blueprints for common standards. The EU strategy should build upon existing data sharing initiatives in the quest for interoperability and the specification of future soft infrastructure agreements (see L. Nagel and D. Lycklama in Designing Data Spaces – The Ecosystem Approach to Competitive Advantage, p. 19; https://link.springer.com/content/pdf/10.1007/978-3-030-93975-5.pdf.)

For the future development of data spaces in light of the new EU regulations, the Data Spaces Support Centre (see DSSC – Data Space Support Centre) will also play a significant role in providing aligned support for common EU data spaces.

In the "European Strategy for Data", the Commission proposed five regulations

AI Act Proposal (AIA-E): Proposed April 2021, legislative procedure ongoing. EU framework for regulating AI; Applies to providers and users of AI.

Data Act Proposal (DA-E): Proposed February 2022, legislative procedure ongoing Obligations of developers + manufacturers of products to facilitate the user's access to data generated during the use. Facilitating switching of data processing services, introducing safeguards, and interoperability standards.

Data Governance Act (DGA): Applicable September 24, 2023. Reuse of data by public sector bodies; framework for data intermediation services + voluntary registration of entities that process data made available for altruistic purposes; European Data Innovation Board.

Digital Markets Act (DMA): Entered into force on May 2, 2023. Regulating internet corporations/ gatekeepers (e.g., social media platforms, search engines). Prohibits practices that make it difficult for users to use non-gatekeeper providers.

Digital Services Act (DSA): Will enter into force on February 16, 2024 (some provisions apply earlier). Protection against illegal content + for users' rights. Applies to intermediary services (e.g., internet access providers, cloud services). Regulations on liability, handling of illegal content, provision of a notice-and-takedown procedure, and regulation of online platforms.

3 Background study on related laws and regulations

In this section we provide thorough details on each related law and regulation in the field. We divide our analysis into seven part, each part representing a related law.

3.1 General Data Protection Regulation (GDPR) [1]

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live and outside of the European Union (EU)1. It was drafted and passed by the European Union (EU) and imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU2. GDPR is designed to give EU citizens more control over their personal data and simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy [2].

The General Data Protection Regulation (Regulation (EU) 2016/679, abbreviated GDPR) is a European Union regulation on Information privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also governs the transfer of personal data outside the EU and EEA. The GDPR's goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business. It supersedes the Data Protection Directive 95/46/EC and, among other things, simplifies the terminology.

The European Parliament and Council of the European Union adopted the GDPR on 14 April 2016, to became effective on 25 May 2018. Because the GDPR is a regulation, rather than a European Union directive, it is directly binding and applicable,[clarification needed : On whom? What does 'directly binding and applicable' mean?] and it provides flexibility for individual member states to modify some provisions of the GDPR.

The regulation became a model for many other laws around the world, including in Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina and Kenya. As of 6 October 2022, the United Kingdom enacted its own law identical to the GDPR despite no longer being an EU member state. The California Consumer Privacy Act (CCPA), adopted on 28 June 2018, has many similarities with the GDPR.

Content

The GDPR 2016 has eleven chapters, concerning general provisions, principles, rights of the data subject, duties of data controllers or processors, transfers of personal data to third countries, supervisory authorities, cooperation among member states, remedies, liability, or penalties for breach of rights, and miscellaneous final provisions. Recital 4 proclaims that ‘processing of personal data should be designed to serve mankind’.

General provisions

The regulation applies if the data controller (an organisation that collects information about living people, whether they are in the EU or not), or processor (an organisation that processes data on behalf of a data controller like cloud service providers), or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply

to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity." (Recital 18)

According to the European Commission, "Personal data is information that relates to an identified or identifiable individual. If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual." The precise definitions of terms such as "personal data", "processing", "data subject", "controller", and "processor" are stated in Article 4 of the Regulation.

The regulation does not purport to apply to the processing of personal data for national security activities or law enforcement of the EU; however, industry groups concerned about facing a potential conflict of laws have questioned whether Article 48[5] of the GDPR could be invoked to seek to prevent a data controller subject to a third country's laws from complying with a legal order from that country's law enforcement, judicial, or national security authorities to disclose to such authorities the personal data of an EU person, regardless of whether the data resides in or out of the EU. Article 48 states that any judgement of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may not be recognised or enforceable in any manner unless based on an international agreement, like a mutual legal assistance treaty in force between the requesting third (non-EU) country and the EU or a member state. The data protection reform package also includes a separate Data Protection Directive for the police and criminal justice sector that provides rules on personal data exchanges at State level, Union level, and international levels.

A single set of rules applies to all EU member states. Each member state establishes an independent supervisory authority (SA) to hear and investigate complaints, sanction administrative offences, etc. SAs in each member state co-operate with other SAs, providing mutual assistance and organising joint operations. If a business has multiple establishments in the EU, it must have a single SA as its "lead authority", based on the location of its "main establishment" where the main processing activities take place. The lead authority thus acts as a "one-stop shop" to supervise all the processing activities of that business throughout the EU (Articles 46–55 of the GDPR). A European Data Protection Board (EDPB) co-ordinates the SAs. EDPB thus replaces the Article 29 Data Protection Working Party. There are exceptions for data processed in an employment context or in national security that still might be subject to individual country regulations (Articles 2(2)(a) and 88 of the GDPR).

Principles

Personal data may not be processed unless there is at least one legal basis to do so. Article 6 states that the lawful purposes are:

a) If the data subject has given consent to the processing of his or her personal data;

b) To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;

c) To comply with a data controller's legal obligations;

d) To protect the vital interests of a data subject or another individual;

e) To perform a task in the public interest or in official authority;

f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

If informed consent is used as the lawful basis for processing, consent must have been explicit for data collected and each purpose data is used for (Article 7; defined in Article 4). Consent must be a specific, freely given, plainly worded, and unambiguous affirmation given by the data subject; an online form which has consent options structured as an opt-out selected by default is a violation of the GDPR, as the consent is not unambiguously affirmed by the user. In addition, multiple types of processing may not be "bundled" together into a single affirmation prompt, as this is not specific to each use of data, and the individual permissions are not freely given. (Recital 32)

Data subjects must be allowed to withdraw this consent at any time, and the process of doing so must not be harder than it was to opt in. (Article 7(3)) A data controller may not refuse service to users who decline consent to processing that is not strictly necessary in order to use the service. (Article 8) Consent for children, defined in the regulation as being less than 16 years old (although with the option for member states to individually make it as low as 13 years old (Article 8(1)), must be given by the child's parent or custodian, and verifiable (Article 8).

If consent to processing was already provided under the Data Protection Directive, a data controller does not have to re-obtain consent if the processing is documented and obtained in compliance with the GDPR's requirements (Recital 171).

Rights of the data subject

Transparency and modalities

Article 12 requires the data controller to provide information to the "data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

Information and access

The right of access (Article 15) is a data subject right. It gives people the right to access their personal data and information about how this personal data is being processed. A data controller must provide, upon request, an overview of the categories of data that are being processed (Article 15(1)(b)) as well as a copy of the actual data (Article 15(3)); furthermore, the data controller has to inform the data subject on details about the processing, such as the purposes of the processing (Article 15(1)(a)), with whom the data is shared (Article 15(1)(c)), and how it acquired the data (Article 15(1)(g)).

A data subject must be able to transfer personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. Data that has been sufficiently anonymised is excluded, but data that has been only de-identified but remains possible to link to the individual in question, such as by providing the relevant identifier, is not. In practice, however, providing such identifiers can be challenging, such as in the case of Apple's Siri, where voice and transcript data is stored with a personal identifier that the manufacturer restricts access to, or in online behavioural targeting, which relies heavily on device fingerprints that can be challenging to capture, send, and verify.

Both data being 'provided' by the data subject and data being 'observed', such as about behaviour, are included. In addition, the data must be provided by the controller in a structured and commonly used standard electronic format. The right to data portability is provided by Article 20 of the GDPR.

Rectification and erasure

A right to be forgotten was replaced by a more limited right of erasure in the version of the GDPR that was adopted by the European Parliament in March 2014 Article 17 provides that the data subject has the right to request erasure of personal data related to them on any one of a number of grounds, including noncompliance with Article 6(1) (lawfulness) that includes a case (f) if the legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data (see also Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González).

Right to object and automated decisions

Article 21 of the GDPR allows an individual to object to processing personal information for marketing or non-service related purposes. This means the data controller must allow an individual the right to stop or prevent controller from processing their personal data.

There are some instances where this objection does not apply. For example, if:

1. Legal or official authority is being carried out

2. "Legitimate interest", where the organisation needs to process data in order to provide the data subject with a service they signed up for

3. A task being carried out for public interest.

GDPR is also clear that the data controller must inform individuals of their right to object from the first communication the controller has with them. This should be clear and separate from any other information the controller is providing and give them their options for how best to object to the processing of their data.

There are instances the controller can refuse a request, in the circumstances that the objection request is "manifestly unfounded" or "excessive", so each case of objection must be looked at individually. Other countries such as Canada are also, following the GDPR, considering legislation to regulate automated decision making under privacy laws, even though there are policy questions as to whether this is the best way to regulate AI.

Controller and processor

Data controllers must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. Firms have the obligation to protect data of employees and consumers to the degree where only the necessary data is extracted with minimum interference with data privacy from employees, consumers, or third parties. Firms should have internal controls and regulations for various departments such as audit, internal controls, and operations. Data subjects have the right to request a portable copy of the data collected by a controller in a common format, as well as the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities consist of regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report data breaches to national supervisory authorities within 72 hours if they have an adverse effect on user privacy. In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

To be able to demonstrate compliance with the GDPR, the data controller must implement measures that meet the principles of data protection by design and by default. Article 25 requires data protection measures to be designed into the development of business processes for products and services. Such measures include pseudonymising personal data, by the controller, as soon as possible (Recital 78). It is the responsibility and the liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller (Recital 74). When data is collected, data subjects must be clearly informed about the extent of data collection, the legal basis for the processing of personal data, how long data is retained, if data is being transferred to a third-party and/or outside the EU, and any automated decision-making that is made on a solely algorithmic basis. Data subjects must be informed of their privacy rights under the GDPR, including their right to revoke consent to data processing at any time, their right to view their personal data and access an overview of how it is being processed, their right to obtain a portable copy of the stored data, their right to erasure of their data under certain circumstances, their right to contest any automated decision-making that was made on a solely algorithmic basis, and their right to file complaints with a Data Protection Authority. As such, the data subject must also be provided with contact details for the data controller and their designated data protection officer, where applicable.

Data protection impact assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the data protection authorities is required for high risks.

Article 25 requires data protection to be designed into the development of business processes for products and services. Privacy settings must therefore be set at a high level by default, and technical and procedural measures shall be taken by the controller to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers shall also implement mechanisms to ensure that personal data is not processed unless necessary for each specific purpose. This is known as data minimisation.

A report by the European Union Agency for Network and Information Security elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe if only the data owner, not the cloud service, holds the decryption keys.

Pseudonymisation

According to the GDPR, pseudonymisation is a required process for stored data that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information (as an alternative to the other option of complete data anonymisation). An example is encryption, which renders the original data unintelligible in a process that cannot be reversed without access to the correct decryption key. The GDPR requires for the additional information (such as the decryption key) to be kept separately from the pseudonymised data.

Another example of pseudonymisation is tokenisation, which is a non-mathematical approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens. While the tokens have no extrinsic or exploitable meaning or value, they allow for specific data to be fully or partially visible for processing and analytics while sensitive information is kept hidden. Tokenisation does not alter the type or length of data, which means it can be processed by legacy systems such as databases that may be sensitive to data length and type. This also requires much

fewer computational resources to process and less storage space in databases than traditionally encrypted data.

Pseudonymisation is a privacy-enhancing technology and is recommended to reduce the risks to the concerned data subjects and also to help controllers and processors to meet their data protection obligations (Recital 28).

Records of processing activities[edit]

According to Article 30, records of processing activities have to be maintained by each organisation matching one of following criteria:

- employing more than 250 people;
- the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects;
- the processing is not occasional;
- processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Such requirements may be modified by each EU country. The records shall be in electronic form and the controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

Records of controller shall contain all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller,[a] the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Records of processor shall contain all of the following information:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

- the categories of processing carried out on behalf of each controller;

- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the

- documentation of suitable safeguards;

- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Security of personal data

Controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate). Data controllers must design information systems with privacy in mind. For instance, using the highest-possible privacy settings by default, so that the datasets are not publicly available by default and cannot be used to identify a subject. No personal data may be processed unless this processing is done under one of the six lawful bases specified by the regulation (consent, contract, public task, vital interest, legitimate interest or legal requirement). When the processing is based on consent the data subject has the right to revoke it at any time.

Article 33 states the data controller is under a legal obligation to notify the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals. There is a maximum of 72 hours after becoming aware of the data breach to make the report. Individuals have to be notified if a high risk of an adverse impact is determined (Article 34). In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach (Article 33). However, the notice to data subjects is not required if the data controller has implemented appropriate technical and organisational protection measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption (Article 34).

Data protection officer [Edit]

Article 37 requires appointment of a data protection officer. If processing is carried out by a public authority (except for courts or independent judicial authorities when acting in their judicial capacity), or if processing operations involve regular and systematic monitoring of data subjects on a large scale, or if processing on a large scale of special categories of data and personal data relating to criminal convictions and offences (Articles 9 and Article 10,]) a data protection officer (DPO)—a person with expert knowledge of data protection law and practices—must be designated to assist the controller or processor in monitoring their internal compliance with the Regulation.

A designated DPO can be a current member of staff of a controller or processor, or the role can be outsourced to an external person or agency through a service contract. In any case, the processing body must make sure that there is no conflict of interest in other roles or interests that a DPO may

hold. The contact details for the DPO must be published by the processing organisation (for example, in a privacy notice) and registered with the supervisory authority.

The DPO is similar to a compliance officer and is also expected to be proficient at managing IT processes, data security (including dealing with cyberattacks) and other critical business continuity issues associated with the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations. The DPO must maintain a living data inventory of all data collected and stored on behalf of the organization. More details on the function and the role of data protection officer were given on 13 December 2016 (revised 5 April 2017) in a guideline document.

Organisations based outside the EU must also appoint an EU-based person as a representative and point of contact for their GDPR obligations (Article 27). This is a distinct role from a DPO, although there is overlap in responsibilities that suggest that this role can also be held by the designated DPO.

Remedies, liability and penalties

Besides the definitions as a criminal offence according to national law following Article 83 GDPR the following sanctions can be imposed:

- a warning in writing in cases of first and non-intentional noncompliance

- regular periodic data protection audits

- a fine up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions (Article 83, Paragraph 4):

o the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39, and 42 and 43

o the obligations of the certification body pursuant to Articles 42 and 43

o the obligations of the monitoring body pursuant to Article 41(4)

- a fine up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions (Article 83, Paragraph 5 & 6):

o the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7, and 9

o the data subjects' rights pursuant to Articles 12 to 22

o the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49

o any obligations pursuant to member state law adopted under Chapter IX

o noncompliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)

Exemptions

These are some cases which are not addressed in the GDPR specifically, thus are treated as exemptions.

- Personal or household activities
- Law enforcement
- National security

When the GDPR was being created, it was strictly created for the regulation of personal data which goes into the hands of companies. What is not covered by the GDPR is non-commercial information or household activities. An example of these household activities may be emails between two high school friends.

Conversely, an entity or more precisely an "enterprise" has to be engaged in "economic activity" to be covered by the GDPR.] Economic activity is defined broadly under European Union competition law.

Applicability outside of the European Union

The GDPR also applies to data controllers and processors outside of the European Economic Area (EEA) if they are engaged in the "offering of goods or services" (regardless of whether a payment is required) to data subjects within the EEA or are monitoring the behaviour of data subjects within the EEA (Article 3(2)). The regulation applies regardless of where the processing takes place. This has been interpreted as intentionally giving GDPR extraterritorial jurisdiction for non-EU establishments if they are doing business with people located in the EU. It is questionable whether the EU or its member states will in practice be able to enforce GDPR against organisations which have no establishment in the EU.

EU Representative

Under Article 27, non-EU establishments subject to GDPR are obliged to have a designee within the European Union, an "EU Representative", to serve as a point of contact for their obligations under the regulation. The EU Representative is the Controller's or Processor's contact person vis-à-vis European privacy supervisors and data subjects, in all matters relating to processing, to ensure compliance with this GDPR. A natural (individual) or moral (corporation) person can play the role of an EU Representative. The non-EU establishment must issue a duly signed document (letter of accreditation) designating a given individual or company as its EU Representative. The said designation can only be given in writing.

An establishment's failure to designate an EU Representative is considered ignorance of the regulation and relevant obligations, which itself is a violation of the GDPR subject to fines of up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater. The intentional or negligent (willful blindness) character of the infringement (failure to designate an EU Representative) may rather constitute aggravating factors.

An establishment does not need to name an EU Representative if they only engage in occasional processing that does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) of GDPR or processing of personal data relating to criminal convictions and offences referred to in Article 10, and such processing is unlikely to result in a risk to the rights and freedoms

of natural persons, taking into account the nature, context, scope and purposes of the processing. Non-EU public authorities and bodies are equally exempted.

Third countries

Chapter V of the GDPR forbids the transfer of the personal data of EU data subjects to countries outside of the EEA — known as third countries — unless appropriate safeguards are imposed, or the third country's data protection regulations are formally considered adequate by the European Commission (Article 45). Binding corporate rules, standard contractual clauses for data protection issued by a Data Processing Agreement (DPA), or a scheme of binding and enforceable commitments by the data controller or processor situated in a third country, are among examples.

United Kingdom implementation

The applicability of GDPR in the United Kingdom is affected by Brexit. Although the United Kingdom formally withdrew from the European Union on 31 January 2020, it remained subject to EU law, including GDPR, until the end of the transition period on 31 December 2020. The United Kingdom granted royal assent to the Data Protection Act 2018 on 23 May 2018, which augmented the GDPR, including aspects of the regulation that are to be determined by national law, and criminal offences for knowingly or recklessly obtaining, redistributing, or retaining personal data without the consent of the data controller.

Under the European Union (Withdrawal) Act 2018, existing and relevant EU law was transposed into local law upon completion of the transition, and the GDPR was amended by statutory instrument to remove certain provisions no longer needed due to the UK's non-membership in the EU. Thereafter, the regulation will be referred to as "UK GDPR". The UK will not restrict the transfer of personal data to countries within the EEA under UK GDPR. However, the UK will become a third country under the EU GDPR, meaning that personal data may not be transferred to the country unless appropriate safeguards are imposed, or the European Commission performs an adequacy decision on the suitability of British data protection legislation (Chapter V). As part of the withdrawal agreement, the European Commission committed to perform an adequacy assessment.

In April 2019, the UK Information Commissioner's Office (ICO) issued a children's code of practice for social networking services when used by minors, enforceable under GDPR, which also includes restrictions on "like" and "streak" mechanisms in order to discourage social media addiction and on the use of this data for processing interests.

In March 2021, Secretary of State for Digital, Culture, Media and Sport Oliver Dowden stated that the UK was exploring divergence from the EU GDPR in order to "[focus] more on the outcomes that we want to have and less on the burdens of the rules imposed on individual businesses".

Misconceptions

Some common misconceptions about GDPR include:

- All processing of personal data requires consent of the data subject.

o In fact, data can be processed without consent if one of the other five lawful bases for processing applies, and obtaining consent may often be inappropriate.

- Individuals have an absolute right to have their data deleted (right to be forgotten)

o Whilst there is an absolute right to opt-out of direct marketing, data controllers can continue to process personal data where they have a lawful basis to do so, as long as the data remain necessary for the purpose for which it was originally collected.

• Removing individuals' names from records takes them out of scope of GDPR

o "Pseudonymous" data where an individual is identified by a number can still be personal data if the data controller is capable of tying that data back to an individual in another way.

• GDPR applies to anyone processing personal data of EU citizens anywhere in the world

o In fact, it applies to non-EU established organizations only where they are processing data of data subjects located in the EU (irrespective of their citizenship) and then only when supplying goods or services to them, or monitoring their behaviour.

Reception

As per a study conducted by Deloitte in 2018, 92% of companies believe they can comply with GDPR in their business practices in the long run.

Companies operating outside of the EU have invested heavily to align their business practices with GDPR. The area of GDPR consent has several implications for businesses who record calls as a matter of practice. A typical disclaimer is not considered sufficient to gain assumed consent to record calls. Additionally, when recording has commenced, should the caller withdraw their consent, then the agent receiving the call must be able to stop a previously started recording and ensure the recording does not get stored.

IT professionals expect that compliance with the GDPR will require additional investment overall: over 80 percent of those surveyed expected GDPR-related spending to be at least US$100,000. The concerns were echoed in a report commissioned by the law firm Baker & McKenzie that found that "around 70 percent of respondents believe that organizations will need to invest additional budget/effort to comply with the consent, data mapping and cross-border data transfer requirements under the GDPR." The total cost for EU companies is estimated at around €200 billion while for US companies the estimate is for $41.7 billion. It has been argued that smaller businesses and startup companies might not have the financial resources to adequately comply with the GDPR, unlike the larger international technology firms (such as Facebook and Google) that the regulation is ostensibly meant to target first and foremost. A lack of knowledge and understanding of the regulations has also been a concern in the lead-up to its adoption. A counter-argument to this has been that companies were made aware of these changes two years prior to them coming into effect and should have had enough time to prepare.

The regulations, including whether an enterprise must have a data protection officer, have been criticized for potential administrative burden and unclear compliance requirements. Although data minimisation is a requirement, with pseudonymisation being one of the possible means, the regulation provides no guidance on how or what constitutes an effective data de-identification scheme, with a grey area on what would be considered as inadequate pseudonymisation subject to Section 5 enforcement actions. There is also concern regarding the implementation of the GDPR in blockchain systems, as the transparent and fixed record of blockchain transactions contradicts the very nature of the GDPR. Many media outlets have commented on the introduction of a "right to explanation" of algorithmic decisions, but legal scholars have since argued that the existence of such a right is highly unclear without judicial tests and is limited at best.

The GDPR has garnered support from businesses who regard it as an opportunity to improve their data management. Mark Zuckerberg has also called it a "very positive step for the Internet", and has called for GDPR-style laws to be adopted in the US. Consumer rights groups such as The European Consumer Organisation are among the most vocal proponents of the legislation. Other supporters have attributed its passage to the whistleblower Edward Snowden. Free software advocate Richard Stallman has praised some aspects of the GDPR but called for additional safeguards to prevent technology companies from "manufacturing consent".

Impact

Academic experts who participated in the formulation of the GDPR wrote that the law "is the most consequential regulatory development in information policy in a generation. The GDPR brings personal data into a complex and protective regulatory regime."

Despite having had at least two years to prepare and do so, many companies and websites changed their privacy policies and features worldwide directly prior to GDPR's implementation, and customarily provided email and other notifications discussing these changes. This was criticised for resulting in a fatiguing number of communications, while experts noted that some reminder emails incorrectly asserted that new consent for data processing had to be obtained for when the GDPR took effect (any previously-obtained consent to processing is valid as long as it met the regulation's requirements). Phishing scams also emerged using falsified versions of GDPR-related emails, and it was also argued that some GDPR notice emails may have actually been sent in violation of anti-spam laws. In March 2019, a provider of compliance software found that many websites operated by EU member state governments contained embedded tracking from ad technology providers.

The deluge of GDPR-related notices also inspired memes, including those surrounding privacy policy notices being delivered by atypical means (such as a Ouija board or Star Wars opening crawl), suggesting that Santa Claus's "naughty or nice" list was a violation, and a recording of excerpts from the regulation by a former BBC Radio 4 Shipping Forecast announcer. A blog, GDPR Hall of Shame, was also created to showcase unusual delivery of GDPR notices, and attempts at compliance that contained egregious violations of the regulation's requirements. Its author remarked that the regulation "has a lot of nitty gritty, in-the-weeds details, but not a lot of information about how to comply", but also acknowledged that businesses had two years to comply, making some of its responses unjustified.

Research indicates that approximately 25% of software vulnerabilities have GDPR implications. Since Article 33 emphasizes breaches, not bugs, security experts advise companies to invest in processes and capabilities to identify vulnerabilities before they can be exploited, including coordinated vulnerability disclosure processes. An investigation of Android apps' privacy policies, data access capabilities, and data access behaviour has shown that numerous apps display a somewhat privacy-friendlier behaviour since the GDPR was implemented, although they still retain most of their data access privileges in their code. An investigation of the Norwegian Consumer Council into the post-GDPR data subject dashboards on social media platforms (such as Google dashboard) has concluded that large social media firms deploy deceptive tactics in order to discourage their customers from sharpening their privacy settings.

On the effective date, some websites began to block visitors from EU countries entirely (including Instapaper, Unroll.me, and Tribune Publishing-owned newspapers, such as the Chicago Tribune and the Los Angeles Times) or redirect them to stripped-down versions of their services (in the case of National Public Radio and USA Today) with limited functionality and/or no advertising so that they will not be liable. Some companies, such as Klout, and several online video games, ceased operations entirely to coincide with its implementation, citing the GDPR as a burden on their continued

operations, especially due to the business model of the former. The volume of online behavioural advertising placements in Europe fell 25–40% on 25 May 2018.

In 2020, two years after the GDPR began its implementation, the European Commission assessed that users across the EU had increased their knowledge about their rights, stating that "69% of the population above the age of 16 in the EU have heard about the GDPR and 71% of people heard about their national data protection authority." The commission also found that privacy has become a competitive quality for companies which consumers are taking into account in their decisionmaking processes.

Enforcement and inconsistency

Facebook and subsidiaries WhatsApp and Instagram, as well as Google LLC (targeting Android), were immediately sued by Max Schrems's non-profit NOYB just hours after midnight on 25 May 2018, for their use of "forced consent". Schrems asserts that both companies violated Article 7(4) by not presenting opt-ins for data processing consent on an individualized basis, and requiring users to consent to all data processing activities (including those not strictly necessary) or would be forbidden from using the services. On 21 January 2019, Google was fined €50 million by the French DPA for showing insufficient control, consent, and transparency over use of personal data for behavioural advertising. In November 2018, following a journalistic investigation into Liviu Dragnea, the Romanian DPA (ANSPDCP) used a GDPR request to demand information on the RISE Project's sources.

In July 2019, the British Information Commissioner's Office issued an intention to fine British Airways a record £183 million (1.5% of turnover) for poor security arrangements that enabled a 2018 web skimming attack affecting around 380,000 transactions. British Airways was ultimately fined a reduced amount of £20m, with the ICO noting that they had "considered both representations from BA and the economic impact of COVID-19 on their business before setting a final penalty".

In December 2019, Politico reported that Ireland and Luxembourg – two smaller EU countries that have had a reputation as a tax havens and (especially in the case of Ireland) as a base for European subsidiaries of U.S. big tech companies – were facing significant backlogs in their investigations of major foreign companies under GDPR, with Ireland citing the complexity of the regulation as a factor. Critics interviewed by Politico also argued that enforcement was also being hampered by varying interpretations between member states, the prioritisation of guidance over enforcement by some authorities, and a lack of cooperation between member states.

In November 2021, Irish Council for Civil Liberties lodged a formal complaint of the Commission that it is in breach of its obligation under EU Law to carefully monitor how Ireland applies the GDPR. Until January 2023, the Commission published a new commitment based on the complaint of ICCL.

While companies are now subject to legal obligations, there are still various inconsistencies in the practical and technical implementation of GDPR. As an example, according to the GDPR's right to access, the companies are obliged to provide data subjects with the data they gather about them. However, in a study on loyalty cards in Germany, companies did not provide the data subjects with the exact information of the purchased articles. One might argue that such companies do not collect the information of the purchased articles, which does not conform with their business models. Therefore, data subjects tend to see that as a GDPR violation. As a result, studies have suggested for a better control through authorities.

According to the GDPR, end-users' consent should be valid, freely given, specific, informed and active. However, the lack of enforceability regarding obtaining lawful consents has been a challenge.

As an example, a 2020 study, showed that the Big Tech, i.e. Google, Amazon, Facebook, Apple, and Microsoft (GAFAM), use dark patterns in their consent obtaining mechanisms, which raises doubts regarding the lawfulness of the acquired consent.

In March 2021, EU member states led by France were reported to be attempting to modify the impact of the privacy regulation in Europe by exempting national security agencies.

After around 160 million Euros in GDPR fines were imposed in 2020, the figure was already over one billion Euros in 2021.

Influence on foreign laws

Mass adoption of these new privacy standards by multinational companies has been cited as an example of the "Brussels effect", a phenomenon wherein European laws and regulations are used as a baseline due to their gravitas.

The U.S. state of California passed the California Consumer Privacy Act on 28 June 2018, taking effect on 1 January 2020; it grants rights to transparency and control over the collection of personal information by companies in a similar means to GDPR. Critics have argued that such laws need to be implemented at the federal level to be effective, as a collection of state-level laws would have varying standards that would complicate compliance. Two other U.S. states have since enacted similar legislation: Virginia passed the Consumer Data Privacy Act on 2 March 2021, and Colorado enacted the Colorado Privacy Act on 8 July 2021.

The Republic of Turkey, a candidate for European Union membership, has adopted the Law on The Protection of Personal Data on 24 March 2016 in compliance with the EU acquis.

In China, the Personal Information Protection Law (PIPL), "China's first comprehensive law designed to regulate online data and protect personal information" came into force in 2021.

Switzerland will also adopt a new data protection law that largely follows EU’s GDPR.

Timeline

- 25 January 2012: The proposal for the GDPR was released.[9]

- 21 October 2013: The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) had its orientation vote.

- 15 December 2015: Negotiations between the European Parliament, Council and Commission (Formal Trilogue meeting) resulted in a joint proposal.

- 17 December 2015: The European Parliament's LIBE Committee voted for the negotiations between the three parties.

- 8 April 2016: Adoption by the Council of the European Union.[146] The only member state voting against was Austria, which argued that the level of data protection in some respects falls short compared to the 1995 directive.[147][148]

- 14 April 2016: Adoption by the European Parliament.[149]

- 24 May 2016: The regulation entered into force, 20 days after its publication in the Official Journal of the European Union.[17]

- 25 May 2018: Its provisions became directly applicable in all member states, two years after the regulations enter into force.[17]

- 20 July 2018: the GDPR became valid in the EEA countries (Iceland, Liechtenstein, and Norway),[150] after the EEA Joint Committee and the three countries agreed to follow the regulation.[151]

EU Digital Single Market

The EU Digital Single Market strategy relates to "digital economy" activities related to businesses and people in the EU. As part of the strategy, the GDPR and the NIS Directive all apply from 25 May 2018. The proposed ePrivacy Regulation was also planned to be applicable from 25 May 2018, but will be delayed for several months. The eIDAS Regulation is also part of the strategy.

In an initial assessment, the European Council has stated that the GDPR should be considered "a prerequisite for the development of future digital policy initiatives".

3.2 Data Act [3]

The DATA Act is a law that aims to make information on federal expenditures more easily accessible and transparent12. It requires federal agencies to report and track their spending data using government-wide standards established by OMB and Treasury34. The DATA Act covers over $3.7 trillion in annual federal spending and links it to federal program activities32. The DATA Act should not be confused with the Data Act of the European Union, which is a different initiative [4].

EGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

(4) ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member

State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) ‘main establishment’ means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

(20) ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

(22) ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) ‘cross-border processing’ means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

(26) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject

for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information. to be provided where personal data are collected from the data subject

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

▼C1

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

▼B

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation,

taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or

extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

▼C1

3. The competent supervisory authority shall submit the draft requirements for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

▼B

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

▼C1

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

▼B

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

▼C1

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met.

▼B

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (2) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. ►C1 The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. ◄ In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

▼C1

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board.

▼B

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic

review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and

information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates

only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

▼C1

(p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

▼B

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's

members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

▼C1

(c) aims to approve the requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);

▼B

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

▼C1

6. The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the

Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the competent supervisory authority referred to in paragraph 1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

▼B

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) ►C1 where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. ◄ The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has

notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

▼C1

2. Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

▼B

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

▼C1

(l) review the practical application of the guidelines, recommendations and best practices;

▼B

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

▼C1

(o) approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);

(p) approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;

▼B

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council (3).

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage

caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

3.3 The Data Governance Act & The Open Data Directive [5]

On 25 November 2020, The European Commission published the Data Governance Act (DGA) in response to the public consultation on the European Strategy for Data. The consultation served as a means to gauge stakeholders' opinions on the data strategy (including open data, data sharing and data spaces), and as input for several planned initiatives around access to, and re-use of, data. A legislative framework on common European data spaces and an implementing act on a list of high-value datasets under the Open Data Directive was part of the consultation as well.

This featured highlight will explore what the results of the public consultation are and delve into the Open Data Directive.

Consultation on the European Strategy for Data

The EU Public Consultation on the European Strategy for Data received contributions from various stakeholders, including SMEs, EU citizens, business associations, academia, research institutes, as well as public authorities. Results from the consultation fall into four categories:

1. The data strategy, of which 97.2% of the 806 respondents confirmed that the EU needs an overarching data strategy to enable the digital transformation of society, with 91.5% agreeing to the following statement:

2. "More data should be available for the common good, for example for improving mobility, delivering personalized medicine, reducing energy consumption and making our society greener."

3. Data governance, including data standardisation, secondary use of data, data donation and data intermediaries. 772 of the 806 respondents answered this section. 90% of the 772 consider data governance mechanisms necessary to capture the enormous potential of data, particularly for cross-sector data use.

4. High-value datasets, with some 761 of the 806 respondents contributed to this section. 82.2% of these respondents answered that a list of high value datasets (available free of charge, with no restrictions and accessible via application programme interfaces) are a good way to ensure that public sector data can have a positive impact on the EU economy and society. High-value datasets are those with a high commercial potential and the ability to accelerate the development of value-increasing information products across the EU.

5. The (self-/co-) regulatory context of cloud computing, where 61% of respondents state that the current cloud market offers technological solutions that businesses need to continue growing and innovating. However, 48% of 444 stakeholders answered that at one point they have experienced problems in the functioning of the cloud market, and 68% of 449 stakeholders expect risks for the

future. Going forward, 59% of responding users and 64% of responding providers state that self-regulation is appropriate to identify best practices to implement EU legislation around cloud computing.

The Open Data Directive

As part of the European Strategy for Data, the Open Data Directive functions as a common legal framework for government-held data (public sector information) and is geared towards two key concepts in the European market: i.e. transparency and fair competition. This directive will be put in place on the national level over the course of the next years and will ultimately:

- Stimulate the publication of dynamic data and the uptake of Application Programme Interfaces (APIs);

- Reduce the exceptions that now enable public bodies to charge more than marginal costs of dissemination for data re-use;

- Extend the scope of the directive to include data held by public undertakings, under a specific set of rules and research data resulting from public funding; and

- Strengthen the transparency requirements for agreements involving public sector information between public and private parties, thereby avoiding exclusive deals.

Furthermore, the directive includes the adoption of a free-of-charge list of high-value datasets by the Commission. The consultation indicates that the need for these types of datasets is high among stakeholders. They will be labelled within a specific thematic categorisation in the Annex to the directive and act as the building blocks for Artificial Intelligence solutions.

High-value datasets will become a more prevalent topic over the next years and the Digital Governance Act as well as the Open Data Directive provide an initial framework for their arrival and implementation.

3.4 Digital Operational Resilience Act (DORA) [6]

The Digital Operational Resilience Act (DORA) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

Why is DORA needed?

The financial sector is increasingly dependent on technology and on tech companies to deliver financial services. This makes financial entities vulnerable to cyber-attacks or incidents.

When not managed properly, ICT risks can lead to disruptions of financial services offered across borders. This in turn, can have an impact on other companies, sectors and even on the rest of the economy, which underlines the importance of the digital operational resilience of the financial sector.

This is where the Digital Operational Resilience Act, or DORA, comes into play.

What does it cover?

- ICT risk management. Principles and requirements on ICT risk management framework
- ICT third-party risk management. Monitoring third-party risk providers. Key contractual provisions
- Digital operational resilience testing. Basic and advanced testing
- ICT-related incidents. General requirements. Reporting of major ICT-related incidents to competent authorities.
- Information sharing. Exchange of information and intelligence on cyber threats.
- Oversight of critical third-party providers Oversight framework for critical ICT third-party providers

Next Steps

The European Supervisory Agencies (ESAs), the European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority, are jointly leading the development of technical standards as required by the DORA Regulation. These are progressing in two tranches, the first of which is published for public consultation by the ESAs between June and September 2023. The second tranche is expected towards the end of the year. These two tranches of technical standards will:

Tranche 1:

- Further specify required elements of financial entity's risk management framework, and, where applicable, a simplified risk management framework
- Further specify the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats
- Further specify outsourcing policy on contractual arrangements with ICT service providers supporting critical or important functions
- Establish standard templates to be used in the register of information on in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

Tranche 2:

- Establish forms and procedures for financial entities to report a major ICT-related incident and to notify significant cyber threats
- Specify further elements for financial entities to determine and assess when sub-contracting ICT services supporting critical or important functions

- Further specify the details of advanced testing of ICT tools, systems and processes based on threat led penetration testing (TLPT) - including criteria to be used to identify those financial entities that are required to perform TLPT

- Harmonise conditions enabling the conduct of oversight of ICT service providers which are

These technical standards are to be developed by the Joint Committee of the ESAs for adoption by the European Commission in January and July 2024.

Pending the adoption of these technical standards, the DORA Regulation itself already contains a lot of useful information on the requirements which financial entities will be required to comply with from January 2025.

Financial entities should be considering steps they will need to take between now and January 2025 to ensure that they can comply with this regulation and support the intended benefits of increased harmonisation of digital operational resilience across the European financial system.

3.5 The NIS2 Directive A high common level of cybersecurity in the EU 7]

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, while the Council agreed its position on 3 December 2021. The co-legislators reached a provisional agreement on the text on 13 May 2022. The political agreement was formally adopted by the Parliament and then the Council in November 2022. It entered into force on 16 January 2023, and Member States now have 21 months, until 17 October 2024, to transpose its measures into national law.

Introduction

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale, cost and sophistication. In 2017, Cybersecurity Ventures forecast that global ransomware damage costs would reach US$20 billion by 2021, 57 times more than the amount in 2015. It alsopredicted that companies would be suffering a ransomware attack every 11 seconds by 2021, up from every 40 seconds in 2016. As a result, businesses have to invest more money to make cyberspace safer for themselves and their customers. Not only companies but also citizens and entire countries have been affected; the first known cyber-attack on a country was mounted on Estonia in April 2007, affecting the online services of banks, media outlets and government bodies for weeks. Since then, many other countries have suffered cyber-attacks, including on critical infrastructure, such as on electric power systems, hospitals or water plants. According to a Eurobarometer survey, about three quarters (76 %) of respondents believe that they are facing an increasing risk of falling victim to

cybercrime. In 2019, about 64 % of the US population experienced a data breach and 88 % of organisations worldwide experienced 'spear-phishing' attempts.

Given the growing number and cost of cyber-attacks, spending on information security is also increasing worldwide. The global security market is currently worth around US$150 billion, a figure that many predict will rise to US$208 billion in 2023 and US$400 billion in 2026.

Critical sectors, such as transport, energy, health and finance, have become increasingly dependent on digital technologies to run their core business. While growing digital connectivity brings enormous opportunities, it also exposes economies and societies to cyber-threats. The number, complexity and scale of cybersecurity incidents are growing, as is their economic and social impact.

The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. Yet, it has also exacerbated existing problems, such as the digital divide, and contributed to a global rise in cybersecurity incidents. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report. Cybersecurity issues are becoming a day-to-day struggle for the EU.

According to monitoring reports from the EU Agency for Network Information Security (ENISA),cybercrime is becoming increasingly monetised, particularly in the case of major cyber-attacks that use ransomware. Likewise, increased e-commerce and cashless payments bring heightened risks of cybercrime attacks and cybersecurity breaches. With payments becoming increasingly cashless, online theft – of money and also of personal data – has been on the rise. An ENISA Threat Landscape 2021 report demonstrates that cyber-attacks are becoming more sophisticated, targeted, widespread and undetected, and concludes that societies face a long road ahead before they can ensure a more secure digital environment. According to Verizon, 86 % of breaches committed in 2019 were financially motivated and 10 % by espionage. About 45 % of breaches featured hacking, 17 % involved malware and 22 % involved phishing. This trend is expected to increase further, in parallel with technological developments such as the proliferation of devices linked to the Internet of Things (IoT). In an increasingly connected world, where 22.3 billion IoT devices are expected to be in use by 2024, the growing challenges in the cybersecurity landscape have led the EU to reflect on how to enhance the protection of its citizens and companies against cyber-threats and attacks.

Existing situation

The first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013. The strategy identified the achievement of cyberresilience and the development of industrial and technological resources for cybersecurity as its key objectives. The Directive on Security of Network and Information Systems across the EU (the NIS Directive), which had to be transposed by Member States by 9 May 2018, represents the first piece of EU-wide legislation on cybersecurity. It provided for legal measures to boost the overall level of cybersecurity in the EU, with a focus on protecting critical infrastructure. Among other things, it established the NIS Cooperation Group, and the network of Computer Security Incident Response Teams (CSIRTs), to ensure both the exchange of information on cybersecurity and cooperation on specific cybersecurity incidents.

In view of the impending deadlines for its transposition into national legislation (by 9 May 2018) and the identification of operators of essential services (by 9 November 2018), the Commission adopted on 13 September 2017 a communication aimed at supporting Member States in their efforts to implement the directive swiftly and coherently across the EU. It introduced an NIS toolkit

providinginformation to Member States on the best practicesrelated to implementing the directive as well as clarifications on some of its provisions.

By 2020, all Member States had communicated to the Commission that they had fully transposedthe directive into their national legislation.

Other legislative initiatives linked to cybersecurity date back to 2017, when the Commission submitted a package of cybersecurity measures to further improve the resilience and incidentresponse capacities of public and private entities, competent authorities and the EU as a whole in the field of cybersecurity and critical infrastructure protection. It also asked for a permanent and enhanced role for the EU cybersecurity agency and the creation of the first EU cybersecurity certification framework, which resulted in the Cybersecurity Act.

Since then, a new EU cybersecurity strategy for 2020-2025 has been adopted, proposing among many things the review of the NIS Directive, the adoption of a new critical entities resilience (CER) directive, a network of security operations centres (SOCs) and new measures to strengthen the EU cyber-diplomacy toolbox. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people.

The threat landscape has changed considerably since the NIS Directive was adopted in 2016, and the scope of the directive needs updating and expanding to meet current risks and future challenges, one such challenge being to ensure that 5G technology is secure. In addition, its transposition and implementation has brought to light inherent flaws in certain provisions or approaches, such as the unclear delimitation of the scope of the directive. Furthermore, since the onset of the coronavirus crisis, the EU economy has grown more dependent on network and information systems than ever before, and sectors and services are increasingly interconnected.

The pandemic has more than confirmed the importance of preparing the EU for the digital decade as well as the need to continually improve cyber-resilience, particularly for those who operate essential services such as healthcare and energy.

Funding for EU cybersecurity initiatives has increased in the 2021-2027 programming period through a mix of instruments such as the Digital Europe Programme, Horizon Europe, the European Defence Fund, and the EU Recovery and Resilience Facility. The EU objective is to reach up to €4.5 billion of combined investment. Notably to go to SMEs under the recently established Cybersecurity Competence Centre and Network of Coordination Centres.

In terms of existing case law, the Court of Justice of the EU in its judgment in Case C-58/08 Vodafone and others has shown the need for establishing clear common rules on the scope of application of the NIS Directive and on harmonising the rules on cybersecurity risk management and incident reporting. Current disparities in this area at the legislative, supervisory, national and EU level are obstacles to the internal market, because entities that engage in cross-border activities face different, and possibly overlapping, regulatory requirements and/or their application, to the detriment of the exercise of their freedoms of establishment and of provision of services.

Parliament's starting position

In a resolution of 3 October 2017 on the fight against cybercrime, in the light of the increasing number of connected appliances, Parliament called for attention to be drawn to the safety of all devices and for action to promote the security-by-design approach. It urged Member States to speed up the setting-up of computer emergency response teams to which businesses and consumers can report malicious emails and websites, as envisaged by the NIS Directive.

In its resolution of 16 January 2016, Towards a Digital Single Market Act, Parliament called for the Commission to put in place a strong cybersecurity agency. More specifically, it called for efforts to be made to improve resilience against cyber-attacks, with an increased role for ENISA.

Council and European Council starting position

In its conclusions of 2 December 2020 on the security of connected devices, the Council encouragedthe Commission to assess the complementary sector-specific regulations that should define what level of cybersecurity should be met by the connected device to ensure that specific security and privacy requirements are put in place for devices with higher security risks.

In its conclusions of 2 October 2020, the Council called for accelerating the deployment of very highcapacity and secure network infrastructures (including fibre and 5G) all over the EU, and for enhancing the EU's ability to protect itself. It furthermore called on the EU and the Member Statesto make full use of the 5G cybersecurity toolbox adopted on 29 January 2020.

In its conclusions of 9 June 2020, the Council welcomed '…the Commission's plans to ensure consistent rules for market operators and facilitate secure, robust and appropriate informationsharing on threats as well as incidents, including through a review of the Directive on security of network and information systems (NIS Directive), to pursue options for improved cyber-resilience and more effective responses to cyber-attacks, particularly on essential economic and societal activities, whilst respecting Member States' competences, including the responsibility for their national security'.

Preparation of the proposal

To underpin the proposal and collect evidence, the Commission ran an open public consultation (OPC), launched stakeholder interviews, country visits, workshops and surveys, carried out a study on NIS investment and an impact assessment, and drew up a roadmap.

The main results of some of the finalised input activities are briefly described below.

Open public consultation

The OPC contributed to the evaluation and impact assessment of the NIS Directive. It included questions targeting citizens, stakeholders and cybersecurity experts. The OPC was carried out over a 12-week period, starting on 7 July 2020 and closing on 2 October 2020. A total of 206 replies were collected online, 182 of which were from respondents located in the EU-27. The hottest topic was the lack of a harmonised approach, resulting in significant inconsistencies in the way Member States draw up lists of operators of essential services (OESs) and digital service providers (DSPs). Consequently, companies of the same type might face different requirements depending on the Member State in which they operate. Likewise, a company might be identified as an OES in one Member State and a DSP in another Member State,1 or as a service provider, thus being excluded from the scope of the NIS Directive in yet another Member State. The responses relating to the identification of OESs suggest that Member States' approaches are often highly heterogeneous. To that end, it was suggested to establish a common set of criteria to ensure a harmonised process of OES identification.

The OPC concluded that some identification practices used by Member States can have a negative impact on the level playing field in the internal market, and potentially render entities more vulnerable to cross-border cyber-threats.

An overwhelming majority of the OPC respondents agreed that common EU rules are needed to address cyber-threats, given that cyber-risks can propagate across borders at high speed. The overall results revealed that OPC respondents on average show significantly more support for the inclusion of public administrations and data centres within the scope of the NIS Directive.

ENISA study on investments

A December 2020 ENISA NIS investments report presents the findings of a survey of 251 organisations of OESs and DSPs from France, Germany, Italy, Spain and Poland, examining their approaches to cybersecurity spending. The survey showed that 82 % of OESs and DSPs find that the NIS Directive has had a positive effect. However, gaps in investment still exist. When comparing organisations from the EU to their US counterparts, data shows that EU organisations allocate on average 41 % less to cybersecurity than their US counterparts.

Impact assessment

The Commission conducted an impact assessment (IA) for the current proposal, comprising three different documents. The IA explored four different policy options for the NIS review, including the baseline option: 0) maintaining the status quo; 1) non-legislative measures to align the transposition; 2) limited changes to the NIS Directive for further harmonisation; and 3) systemic and structural changes to the NIS Directive. Option 1 was discarded at an early stage, as it does not depart considerably from the status quo. The analysis led to the conclusion that option 3 – systemic and structural changes to the NIS framework – is the preferred one. Option 3 would envisage a more fundamental shift of approach towards covering a wider segment of the economies across the EU, yet with a more focused supervision targeting proportionally big and key companies, while clearly determining the scope of application. It would also streamline and further harmonise companies' security-related obligations, create a more effective setting for operational aspects, establish a clear basis for shared responsibilities and accountability of the entities concerned, and incentivise information sharing.

The IA was submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020 and received its feedback in the form of a positive opinion with comments on 20 November 2020. The RSB insisted that the IA should clearly distinguish between 'essential' and 'important' sectors, clarify the criteria for establishing these categories, and consider whether alternative approaches are possible. It asked the Commission to expand on whether the definition of sectoral coverage risks shifting the danger of exposure to other sectors and to analyse how the choice of sectors could be made future proof.

The RSB also observed that the IA should reinforce the problem analysis to better focus on the problems the directive aims to solve. Furthermore, the IA should include a more complete set of options on reporting, supervision and crisis response. It should include ways to interact with the linked European Critical Infrastructure Directive, which is also under revision. Finally, the IA should strengthen the analysis of compliance costs, especially for medium-sized enterprises.

The initial appraisal drawn up by EPRS provides a detailed analysis of the IA. According to it, the NIS2 proposal appears to follow the general considerations of the IA. The preferred option identified in the IA is at the core of the proposal. The monitoring provisions however do not appear to have been laid out in the proposal with the same level of detail as in the IA.

NIS evaluation

Article 23 of the NIS Directive requiresthe Commission to review the functioning of the NIS Directive periodically. As part of its key policy objective to make 'Europe fit for the digital age' as well as in line with the objectives of the security union, the Commission announced in its work programme 2020 that it would conduct the review by the end of 2020.

On 25 June 2020, the Commission published a combined evaluation roadmap/inception impact assessment on the revision of the NIS Directive, according to which it planned to 'evaluate the functioning of the NIS Directive based on the level of security of network and information systems in the Member States'. The Commission underlined that in addition to the requirement under Article 23 of the NIS Directive, the revision was 'further justified by the sudden increase in the dependence on information technology during the Covid-19 crisis'. The Commission stated that 'depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union'.

The Commission evaluation analysed the NIS directive for its relevance, EU added value, coherence, effectiveness and efficiency. Its main findings were that the scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to: i) increased digitalisation in recent years and a higher degree of interconnectedness; and ii) the scope of the NIS Directive no longer reflecting all digitalised sectors providing key services to the economy and society as a whole.

Furthermore, the evaluation concluded that the NIS Directive does not provide sufficient clarity as regards the scope criteria for OESs or the national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in some Member States and are therefore not required to put in place security measures and report incidents. For example, certain major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to implement the resulting security measures, while in another Member State almost every single healthcare provider is covered by the NIS security requirements.

The NIS Directive afforded Member States broad discretion when laying down security and incident reporting requirements for OESs. The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways, creating an additional burden for companies operating in more than one Member State.

The supervision and enforcement regime of the NIS Directive is ineffective. The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber-resilience among Member States.

Member States do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. This is also the case for information-sharing among private entities and for the engagement between the EU level cooperation structures and private entities.

The changes the proposal would bring

The Commission presented on 16 December 2020 a proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), which would repeal and replace the existing NIS Directive (NIS1). The proposed directive aims to tackle the limitations of the current NIS1 regime. The legal basis for both NIS1 and the proposed NIS2 is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules.

The proposed expansion of the scope covered by NIS2, which would effectively oblige more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Overall, the NIS2 proposal sets itself three general objectives:

 Reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive, by further aligning i) the de facto scope; ii) the security and incident reporting requirements; iii) the provisions governing national supervision and enforcement; and iv) the capabilities of the Member States' relevant competent authorities. The proposal includes a list of seven key elements that all companies must address or implement as part of the measures they take, including incident response, supply chain security, encryption and vulnerability disclosure. In addition, the proposal envisages a two-stage approach to incident reporting. Affected companies have 24 hours from when they first become aware of an incident to submit an initial report, followed by a final report no later than one month later. Regarding enforcement, it establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk management or their reporting obligations laid down in the NIS Directive. These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher).

 Improve the level of joint situational awareness and the collective capability to prepare and respond, by i) taking measures to increase the level of trust between competent authorities; ii) by sharing more information; and iii) setting rules and procedures in the event of a large-scale incident or crisis. The proposed new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, appropriate planning and more EU cooperation. The revised directive would establish an EU crisis management framework, requiring Member States to adopt a plan and designate national competent authorities responsible for participating in the response to cybersecurity incidents and crises at the EU level. The proposed directive would establish an EUCyber Crises Liaison Organisation Network (EU-CyCLONe) to support the coordinated management of EU-wide cybersecurity incidents, as well as to ensure the regular exchange of information. The proposed directive would also strengthen the role of the NIS Cooperation Group in making decisions and increasing cooperation between Member States. Member States would still be required to adopt a national cybersecurity strategy and to designate one or more national competent authorities to supervise compliance with the directive; and to designate CSIRTs to handle incident notifications and single points of contact (SPOC) to act as a liaison point with other Member States.

In order to ensure consistency and coherence with related EU legislation, the NIS Directive review in particular takes into account the following three Commission initiatives:

 the review of the Resilience of Critical Entities (CER) Directive, which was proposed alongside the NIS2 proposal, with the objective of improving the resilience of critical entities against physical threats in a large number of sectors. The proposal expands both the scope and depth of the current 2008 directive, including the coverage of 10 sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space;

 the initiative on a digital operational resilience act for the financial sector (DORA);

 the initiative on a network code on cybersecurity with sector-specific rules for cross-border electricity flows (see snapshot analysis from the SPEAR project).

As regards the financial sector, the DORA proposal would provide legal clarity on whether and how digital operational provisions apply, especially to cross-border financial entities, and it would eliminate the need for Member States to individually improve rules, standards and expectations regarding operational resilience and cybersecurity as a response to the current limited coverage of EU rules and the general nature of the NIS1 Directive. At the same time, it is important to maintain a strong relationship for the exchange of information between the financial sector and the other sectors covered by NIS2. To that end, under the DORA proposal, all financial supervisors, the European supervisory authorities (ESAs) for the financial sector and the financial sector-related national competent authorities would be able to participate in the discussions of the NIS Cooperation Group, and to exchange information and cooperate with the single points of contact and with the national CSIRTs under NIS2. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies, and national CSIRTs may cover the financial sector in their activities.

Furthermore, the Commission has aligned the scope in the NIS2 proposal with the proposal for a review of the CER Directive.

As regards ENISA, it would see increased responsibilities within its existing mandate, which involves overseeing the implementation of the NIS. ENISA would be tasked to prepare a report every two years on the state of cybersecurity in the EU and to maintain a European vulnerability registry providing access to information on the vulnerabilities of ICT products and services disclosed on a voluntary basis by essential and important entities and their ICT suppliers. At the same time, ENISA would be required to create and maintain a registry, in which certain types of entities including domain name system service providers, top level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, as well as online marketplaces, online search engines and social networking platforms would notify where they are established in the EU. This is to ensure that such entities do not face a multitude of different legal requirements, given that they provide services across borders to a particularly high extent.

To address key supply chain risks and to assist entities in managing cybersecurity risks related to the ICT supply chain, the NIS Cooperation Group, together with the Commission and ENISA, would be tasked to carry out a coordinated risk assessment per sector of critical ICT services, systems, or products including relevant threats and vulnerabilities. The supply chain risk assessments would consider both technical factors (hardware- or software-related) and, where relevant, non-technical factors (such as suppliers being subject to interference by a non-EU country or state-backed players). This approach largely builds on the previous work of the Commission and the NIS Cooperation Group on the security of 5G networks. The Commission published on 29 January 2020 the 5G risk management toolbox, which listed measures to mitigate the security threats associated with 5G networks. Among others, the EU 5G risk assessment identified security risks related to 5G networks and the 5G supply chain at the EU level. To ensure that entities comply with their obligations addressing ICT supply chain security, the new directive would enable Member States to require essential and important entities to certify specific ICT products, services and processes under the EU Cybersecurity Act. In this context, the draft directive would empower the Commission to lay down which categories of essential entities (due to their criticality) would be required to obtain certification.

The European Electronic Communications Code (EECC) regulates since December 2020 the security of telecoms providers when they are providing electronic communications services in the EU. However, telecoms providers are covered by the current NIS framework if they provide nontelecoms services that fall within the scope of the directive, i.e. cloud computing services. The proposed directive would therefore repeal the corresponding EECC security provisions and entirely regulate the security of telecoms providers, also in cases where they are providing ECS-related services. The same would apply to the security provisions for trust service providers currently found in the eIDAS Regulation.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on the proposal during its plenary session of 27-28 April 2021.

The EESC notes that some of the provisions in both the NIS2 and CER proposals overlap, as they are closely linked and complementary. The EESC therefore calls for the possibility of combining the two proposals to form one single text. Furthermore, given the relevance and sensitivity of the objectives pursued by the two proposals, it finds that a regulation would have been preferable to a directive.

In addition, the EESC points out that clearer guidelines are needed for distinguishing between 'essential' and 'important' entities, and that the respective requirements to be met should be more precisely defined.

Finally, the EESC agrees that ENISA plays a key role in the overall European institutional and operational cybersecurity system. Thus, in addition to the proposed two-yearly report on the state of cybersecurity in the Union, itshould also publish regular, up-to-date information on cybersecurity incidents and sector-specific warnings online.

The European Committee of the Regions (CoR) has not prepared an opinion on the proposal.

National parliaments

The subsidiarity deadline for the submission of reasoned opinions was 17 March 2021. No national parliament submitted any reasoned opinion.

Stakeholder views

From 25 June 2020 to 13 August 2020, all interested stakeholders could provide feedback on the inception impact assessment and roadmap on a dedicated Commission webpage. A total of 42 responses were received from stakeholders, the private sector, research organisations and citizens from the EU and internationally. Stakeholders broadly pointed to the current fragmentation in the implementation of NIS at the national level, particularly regarding OESs and DSPs. They furthermore emphasised the need to improve EU-level coordination of cyber-attack responses and with other related EU legislation.

The GSMA mobile association strongly recommends that the Commission address the shortcomings and persisting inefficiencies in the NIS Directive by: including software and hardware providers in the scope of the NIS, to ensure robust end-to-end security; reducing red tape and fragmentation, by streamlining processes, security requirements and incident notifications obligations; and improving harmonisation and consistency for providers of Electronic Communications Services, by closely aligning the NIS Directive with other legal instruments (the Cybersecurity Act, the EECC and the European Critical Infrastructure (ECI) Directive).

Eurosmart, the association representing the European digital security industry, believes that 'DSPs should use physical infrastructure exclusively located in Europe. The NIS Directive should leverage the European certification schemes created in the framework of the Cybersecurity Act (CSA) to demonstrate the ability of OES and DSP to meet a high level of protection. Following a risk-based approach, certification of highly critical products must be done at a level 'High' pursuant to the CSA. Security certificate at level 'High' ensures continuous monitoring and maintenance of the certification scheme by a community of recognised experts from the industry. It is the only way to ensure "the state of the art" of security for critical infrastructures'.

The Software Alliance (BSA) states that the general spirit of the existing provisions should be kept, but with a better level of harmonisation and implementation, in particular with regard to service definitions, thresholds, reporting modalities, and the categories of (sub-)sectors recognised as OESs and DSPs across the EU. With regard to the call to expand the scope of the NIS to software products, the BSA also underlines that the sector is already covered by force of the inclusion of cloud services in Annex III, notably through the 'software as a service' principle. For the very limited cases where software would not be delivered or serviced through the cloud (i.e. when embedded), the incidentreporting obligations would be irrelevant, as the manufacturer would not have the visibility of the incident affecting that specific piece of software.

Digital Europe, the industry association, believes that the current NIS scope should be maintained. The review should, however, ensure that Member States are more closely aligned in defining OESs and DSPs to avoid fragmentation.

BEUC, the European consumer association, states that the scope of the NIS is not broad enough, especially when it comes to DSPs. As regards OESs, the discrepancies in their selection criteria has created legal fragmentation in the EU.

The European Data Protection Supervisor (EDPS) published an opinion on the cybersecurity strategy and the NIS 2 Directive on 11 March 2021 in which, among other things, he issues specific recommendations to ensure that the proposal correctly and effectively complements existing Union legislation on personal data protection, in particular the GDPR and the ePrivacy Directive. He also asks to clarify the different use of the terms 'cybersecurity' and 'security of network and information systems' across the text: to use the term 'cybersecurity' in general, and the term 'security of network and information systems' only for technical purposes when the context allows it.

The Body of European Regulators for Electronic Communications (BEREC) has published an opinion on 19 May 2021, on the NIS2 proposal recommending that the security of the telecoms sector should continue to be regulated under the EECC. According to BEREC, including the telecoms sector under the scope of NIS2 risks reducing the security level already established through sector-specific regulatory practice since the Framework Directive came into effect in 2009.

Legislative process

In the European Parliament, the Committee on Industry, Research and Energy (ITRE) was assigned the file (rapporteur: Bart Groothuis, Renew, the Netherlands). The Committees on Foreign Affairs (AFET), on Internal Market and Consumer Protection (IMCO), on Transport and Tourism (TRAN) and on Civil Liberties, Justice and Home Affairs (LIBE) all submitted opinions.

On 13 April 2021, the European Commission presented the legislative proposal to Parliament's lead committee, ITRE. MEPs welcomed the proposed review of NIS. The most common concern raised by MEPs was about its compatibility with other proposed or existing EU legislation, including DORA, CER, the Cybersecurity Act, the EECC and the GDPR.

The ITRE draft report was published on 3 May 2021, and the four committee opinions were adopted in July 2021. The ITRE committee adopted its report on 28 October 2021, with 70 votes in favour to 3 against, with 1 abstention. MEPs also voted to open trilogue negotiations with Council, with this mandate confirmed in plenary in November.

The report calls for tighter cybersecurity obligations in terms of risk management, reporting obligations and information-sharing. It aims to lower the administrative burden and to improve

cybersecurity incident reporting. In addition, the report states that EU countries would have to meet stricter supervisory and enforcement measures, and harmonise their sanctions regimes.

The report also states that the Commission should ensure that appropriate guidance is given to all micro- and small enterprises falling within the scope of the NIS2 Directive. The report also supports policies promoting the use of open-source cybersecurity tools, which are of particular importance for SMEs as they face significant costs for implementing cybersecurity tools.

Among other things, the rapporteur added the notion of 'active defence' 5 in his draft report. The report as adopted says that Member States should adopt policies on the promotion of active cyberdefence as part of their national cybersecurity strategies.

The report intends to broaden the sectorial scope to also include academic, knowledge and research institutions which had been left outside the scope of NIS2 by the Commission, while many national cybersecurity strategies cover them.

In June 2021, the Council took stock of progress on NIS2. One of its concerns related to the interaction of NIS2 with sectoral legislation, in particular CER and DORA. During the discussions, most Member States stated that it was imperative to view NIS2 as the horizontal framework for cybersecurity in the EU and that it should serve as a baseline standard for minimum harmonisation of all relevant sectoral legislation in this field. Other concerns raised related to the significant expansion of the scope of the revised rules, the size-cap criteria as the sole element to be considered when identifying essential and important entities to be covered, the proposed legal basis (i.e. single market), and national security concerns.

The Council adopted its negotiating position on 3 December 2021. Compared to the initial proposal for NIS2, the Council introduced a number of significant changes. For instance it introduced additional criteria to determine the entities to be covered by NIS2, excluding from its scope entities operating in defence and national security, public security, law enforcement and the judiciary, as well as parliaments and central banks. It aligned the text with other related proposed legislation, such as the CER Directive and DORA. Furthermore, it simplified the incident-reporting obligations, to avoid over-reporting, and extended the period for Member States to transpose NIS2 into national law to two years, instead of 18 months.

nterinstitutional trilogue negotiations started on 13 January 2022 and a second meeting took place on 17 February. On 13 May, during the third trilogue meeting, the Parliament and Council reached a political agreement. The revised directive sets out minimum rules for a regulatory framework, and lays down cooperation mechanisms among relevant authorities in each Member State. It expands the list of sectors and activities subject to cybersecurity obligations, and improves their enforcement, providing for remedies and sanctions which would vary between essential services and important entities. Parliament negotiators had insisted on the need for clear and precise rules for companies. The reporting obligations have been simplified and streamlined to give entities more time to report than the initial 24 hours proposed by the Commission. This is in order to avoid overreporting and creating an excessive burden on the entities covered. The text has been aligned with sector-specific legislation, in particular with the DORA Regulation and the CER Directive, to provide legal clarity and ensure coherence.

The NIS2 directive would introduce a size-cap rule for determining which entities meet the criteria to qualify as operators of essential services and important entities. This means that all medium-sized and large entities operating within the sectors covered by the directive or providing services covered by the directive would fall within its scope. The co-legislators maintain this general rule but with additional provisions to ensure proportionality and clear-cut criticality criteria for determining them.

Such entities would fall under the jurisdiction of the Member State in which they are established, not of the Member State in which they provide their services.

The directive would also formally establish the EU-CyCLONe network, which will support the coordination and management of large-scale incidents.

In addition, a voluntary peer-learning mechanism would be established to support learning from good practice.

As demanded by the Council, the directive would not apply to entities carrying out activities in areas such as defence and national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope. However, as demanded by the Parliament it will apply to public administration entities at central and regional level. In addition, Member States may also decide that it applies to entities at local level.

The political agreement was endorsed by the ITRE committee on 13 July 2022, and then adopted by Parliament in plenary on 10 November 2022, with 577 votes in favour, 6 against and 31 abstentions. The text was then adopted by the Council on 28 November 2022 and signed by both co-legislators on 14 December 2022. It was published in the Official Journal on 27 December 2022, and entered into force on 16 January 2023. Member States have 21 months – until 17 October 2024 – to transpose the directive into national law.

EP SUPPORTING ANALYSIS

Zygierewicz A., Directive on security of network and information systems (NIS Directive), Implementation appraisal briefing, EPRS, European Parliament, November 2020.

Kononenko V., Improving the common level of cybersecurity across the EU, Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, February 2021.

Erbach G. with O'Shea J., Cybersecurity of critical energy infrastructure, Briefing, EPRS, European Parliament, October 2019.

Negreiro M., ENISA and a new cybersecurity act, Briefing, EPRS, European Parliament, July 2019.

Negreiro M. with Belluomini A., The new European cybersecurity competence centre and network, Briefing, EPRS, European Parliament, July 2020.

OTHER SOURCES

High common level of cybersecurity across the Union – NIS 2 Directive, European Parliament Legislative Observatory.

Challenges to effective EU cybersecurity policy, European Court of Auditors (ECA) Briefing Paper, March 2019.

Report assessing the consistency of the approaches in the identification of operators of essential services, European Commission, 2020.

Internet organised crime threat assessment (IOCTA) 2020, Europol, 2020.

PSD3/PSR + MIFID II + 4AMLD

QuickTake

On 28 June 2023, the European Commission (the Commission) published a package of legislative proposals to propel payments and the wider financial services sector further into the digital age. Since the introduction of the EU's second Payments Services Directive (PSD2) almost eight years ago, the EU has witnessed a steady change in the retail payment services market. Plastic cards issued by brick-and-mortar banks have in part been replaced by new non-bank issuers and BigTechs creating mobile payment services enabling contactless payments. This trend, including new digital payment solutions, the proliferation of payment service offerings as well as new market entries, has increasingly brought to light the limits of the current legislative and regulatory framework.

More importantly, different national implementations of PSD2 and administrative practises of national competent authorities (NCAs) across EU Member States led, in part, to goldplating, exercise of national options and discretions leading to differing interpretations of the scope of regulated payment services (PSPs) and application of exclusions from the authorisation obligation as well as difficulties for new applicants and existing firms to comply with the "local" implementation and supervision of PSD2 across the EU-27. As a result, a certain degree of industry uncertainty and reduced regulatory clarity for firms operating across the EU followed for certain business models, products and services. Equally, the PSD2's aims on "open banking" remained constrained by some of these interpretative barriers both for regulated firms and third-party providers (3TP).

Correspondingly, the EU's 'Payments Services Package'Show Footnote comprised of (i) the third Payment Services Directive (PSD3)Show Footnote replacing PSD2 (and merging in EMD2 – see below), as supplemented by (ii) a new EU Payment Services Regulation (PSR)Show Footnote and (iii) a Regulation on a framework for Financial Data Access (FIDAR) comprehensively reforms but equally expands the existing PSD2/EMD2 framework while at the same time establishing greater harmonisation. The PSR's and FIDAR's provisions notably open the scope of 3TP's access to existing but also new types of accounts and financial products thus driving open banking to more "open finance".Show Footnote Moreover, a number of requirements set out in PSD2's regulatory technical standards (RTS) (i.e. Level 2 rules subject to local divergences) have been moved into the PSR so as to apply in a uniform manner. The new Payment Services Package will have its own implementing technical standards and RTS to cover items previously covered in PSD2/EMD2 as well as new areas. Further coverage on this will be made available as such drafts and final versions are made available.

When taken collectively EU Payment Services Package's reforms aim, beyond improving harmonisation of rules and how they are supervised, to (a) further improve consumer protection and competition in electronic payments, while (b) further empowering consumers to share their data in a manner which is secure and (c) facilitate users' access a wider range of better and cheaper financial products and services and thus improve competition and innovation.

The Commission's revised proposals will need to be considered by the European Parliament and the Council (as the EU's co-legislators). The majority of the amendments are unlikely to take effect before 2025, i.e., 10 years after PSD2's adoption, but many PSPs may want to take preparatory steps ahead of that deadline with some PSD 2 and EMD 2 existing firms having to reapply for licenses and the majority needing to update not only client and counterparty facing documentation (contractual and otherwise) but equally amending existing and introducing new policies, procedures as well as systems and controls to meet the requirements and supervisory expectations of these changes as well as concurrent related EU reforms on (digital) operational resilience.

This Client Alert from PwC Legal's EU RegCORE provides a focused overview of how the co-legislators are aiming to modernise payment services across the EU as well as how an opening of financial services data is envisaged. How are the proposals embracing the new payment services

landscape and how are they incorporating aspects of and superseding prior legislation? Our EU RegCORE team has laid out what to expect and which aspects to monitor as the legislative process moves forward. Readers of this Client Alert may want to refer to related coverage in our "payments services" series in particular how other reforms (including CESOP) may impact client facing documentation and authorised target operating models.

Key aims

The Commission's proposals focus on revising the PSD2 (and merging these with EMD2 as discussed below) into a single legal framework comprised (i) of the PSD3, which, as an EU Directive, will be transposed by Member States into national law and (ii) the associated PSR which will become directly applicable in the Member States. This approach aims to provide greater certainty, consistency and ultimately reduction in barriers and fragmentation.

In addition, the Commission also published a legislative proposal for a financial data access in the form of FIDAR, which seeks to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts. Its main features include the introduction of stipulations for specialised data access interfaces and the elimination of the need for banks to support dual access interfaces. This is an important step forward in enabling full 'open finance' beyond PSD2 pushing 'open banking'. The major changes of these proposals can be summarised in four goals:

1. Strengthening user protection and confidence in payments including by greater combatting of fraud;

2. Improving the competitiveness of open banking;Show Footnote

3. Harmonising enforcement and implementation across EU Member States; and

4. To improve access to payment systems and bank accounts for non-bank PSPs.

The four major objectives of this comprehensive legislative overhaul, as stated above, are pursued via a wide-ranging "package of preferred options" laying down a roadmap to that end. Accordingly, these options generally seek to improve the application of a strong customer authentication (SCA) against criteria included in the PSR, shifting of liability to PSPs corresponding to their augmented role and competencies and requiring the creation of dedicated data access interfaces and "permission dashboards" for payment services users (PSUs).

3.6 The PSD3 and PSR in detail [8]

The existing regulatory framework applicable to authorisation and supervision of payment institutions and e-money institutions (EMIs) currently anchored in PSD2 and the second E-Money Directive (EMD2) will be merged into a single rule book comprised of PSD3 and PSR. Accordingly, EMIs will become a subcategory of PSPs under the proposed framework with a more harmonised authorisation and common supervision process. The Commission also introduces a new definition of "electronic money services" to include e-money issuance, payment account maintenance and transfer of e-money. PSD2's scope of application and exceptions from the authorisation obligation are rehoused to the PSR so as to standardise the EU payment services regulatory framework across the EU.

Summary of key reforms

As for the modernisation of the PSD 2 – which will become PSD 3 – alongside the new PSR, the legislative proposals focus on the following reforms:

Combating and mitigating payment fraud

Allowing PSPs to:

1. voluntarily communicate and share fraud-related information between themselves;

2. increasing consumers' awareness;

3. strengthening customer authentication and SCA rules; and

4. extending refund rights of consumers who fall victim to fraud and making a system for checking alignment of payees' IBAN numbers with their account names mandatory for all credit transfers.

Improving consumer rights

By improving, inter alia, transparency on consumer account statements in cases where their funds are temporarily blocked as well as providing more transparent information on ATM charges. The contractual requirements that PSPs needed to comply with under PSD2 are moved to PSR which presses forward more harmonisation but contains more specific provisions that affect the contents of the framework contracts, termination rights of customers, notice periods, availability of alternative dispute resolution procedures as well as prohibitions on PSPs unilaterally increasing spending limits as well as extension of surcharge bans to all credit transfers and direct debits (beyond current PSD 2 coverage). Such changes, along with various other changes affecting reporting, such as CESOP (see separate coverage from us) will likely require comprehensive changes to client and customer facing documentation i.e., in contracts and otherwise.

Equally, the European Banking Authority (EBA) will be granted product intervention powers.

Furthering the level playing field between banks and non-banks

By allowing non-bank payment providers – in particular – access to all EU payment schemes, with appropriate safeguards and securing those providers' rights to a bank account.

Improve the functioning of open banking

By removing remaining obstacles to the provision of open banking services and improving customers' control over their payment data and thereby enabling new innovative services and new forms of 3TPs to enter the market and move open banking to open finance.

Improve the availability of cash in shops and via ATMs

By allowing retailers to provide cash services to customers without the requirement of a purchase and clarifying the rules for independent ATM operators.

Strengthening harmonisation and enforcement

By upscaling EU-level rulemaking and enacting most payment rules in a directly applicable regulation and reinforcing provisions on implementation and penalties.

Changes to definitions and exclusions

Some key changes are set out in more harmonised definitions and exclusions (including the widely-used limited network exclusion (LNE) under PSD2), thus aiming to reduce fragmentation of NCA's interpretation and supervisory approaches. This includes:

• Revising the current definition of a "payment instrument" under PSD2 that refers to "personalised devices" used in order to initiate a payment order, was a cause for a lot of confusing interpretations across the EU given that NCAs were frequently seeing high level of personalisation of the instrument as a necessary characteristic. The new definition of payment instrument, contained in both PSD3 and PSR, now refers to all "individualised instruments", clarifying that even not fully personalised instruments (like prepaid cards with customers' name on them) can fall under the definition of a regulated payment instrument;

• Amending the definition of a "payment account" by clarifying that the determining criterion for the categorisation of an account as payment account lies in the ability of the customer to perform daily payment transactions from such an account. That being said, the Commission stresses that structures that require another intermediary account for execution of payment transactions from or to third parties should not fall under the definition of a payment account; and

• The exclusion for "commercial agents" was amendedShow Footnote but this will then require such persons to contractually document the framework on which they conclude the sale or purchase of goods and/or services on behalf of the payer or the payee. In contrast, the Commission is using the present reforms to clarify that e-commerce platforms that act as commercial agents for individual buyers and sellers may not rely on the commercial agent exclusion;

• The exclusion for technical service providers is also subject to further clarification in that pass-through wallets including those that use the digitalisation and/or tokenisation of an existing payment instrument are themselves not a payment instrument for purposes of PSD3 but instead a payment application which effectively means the operators of such payment application are unlikely to be subject to a licensing obligation;

• The widely-used LNE will be supplemented by specific forthcoming criteria that set out clear rules upon when the LNE can be used.

Services of issuing of payment instruments and of acquiring payment transactions, which were listed together under PSD2, are listed now separately under proposed PSR/PSD3 framework. Since joint listing of these two services under PSD2 was a cause for a lot of confusion in the industry, the Commission has decided to list them separately now by emphasising that that the issuing and acquiring services may be offered separately by PSPs.

Changes to authorisation and supervision matters

What remains unchanged, under the current proposals, relative to PSD2 are the authorisation application procedures and control of shareholding as well as the provisions regarding agents, branches, and outsourcing. The regulation of cross-border provision of services by PSPs and the supervision of such services likewise remain broadly unchanged.

Moreover, the PSD3 and PSR do not materially alter the current list of payment services. However, existing PSD2 and EMD2 firms are required (under current drafting of the proposals) to reapply for a licence under the new PSD3/PSR regime within 24 months of PSD3 coming into force in order to rely on 'grandfathering provisions" allowing firms' existing licenses to remain valid for 30 months

after PSD 3 enters into force. Affected firms will want to engage proactively with their professional advisors to forward-plan that project as both the world of payments but financial services regulation generally has changed considerably since 2015 and merely updating application materials as submitted previously will not be sufficient.

In addition, among some further reforms in the legislative proposals are a new requirement for PSP (re-)applicants to submit a winding-up plan as part of the licensing procedure. This is in keeping with practice and supervisory expectations that have long existed in other parts of regulated financial services and applicants seeking authorisation. The same is true in the new requirement that PSPs need to provide an overview of the EU jurisdictions where they are submitting or planning to submit an application for an authorisation.

Equally, business continuity plans of PSPs must comply with Regulation (EU) 2022/2554) (DORA) – see our standalone coverage on this. As part of this greater focus on (digital) operational resilience, PSP's (re-)applicants need to also submit a detailed risk assessment, including the risk of fraud and illegal use of sensitive and personal data, accompanied with details of other measures set out in the PSR on the sharing of fraud-related data.

Moreover, safeguarding rules for payment institutions remain largely unchanged under the proposal with the exception of the possibility of safeguarding in an account of a central bank – at the discretion of the latter – in order to extend the options for PSPs to that end as well as the introduction that payment institutions must endeavour to avoid concentration risk in safeguarded funds. To this end, the EBA is tasked with developing RTS on risk management of safeguarded funds as well as guidelines on more detailed provisions regarding internal governance of payment institution. The EBA will also receive product intervention powers.

The role of the EBA is also enhanced proportionally to the digital leap endeavoured in the proposals in that it will continue to maintain, alongside the Member States, a register of authorised payment institutions as well as to develop a list of machine-readable payment initiation services providers and account information service providers. Specific provisions for the clarification of the cooperation between NCAs are also detailed in the proposals. Notably, NCAs are permitted to request assistance of EBA in solving possible disagreements between NCAs to this extent. It is also conceivable that the EBA will make greater use of common supervisory actions through coordinating NCAs' thematic reviews and on-site inspections of persons in-scope of the new EU Payment Services Package.

Importantly, under the (current) PSD3 proposal, PSPs which only carry out account information services are subject only to a registration requirement as opposed to full-fledged authorisation.Show Footnote In the context of supervision of PSPs, the proposals acknowledge that payment initiation service providers and account information service providers may hold initial capital (EUR 50,000) instead of maintaining professional indemnity insurance coverage, considering that the requirement to hold a professional indemnity insurance at the licensing stage may indeed prove difficult to fulfil when taking into account previous experience. On a similar note, possible methods for own funds calculation remains unchanged, either for payment institutions covered by PSD2 or for former electronic money institutions.Show Footnote

Finally, a further clarification is set out for de minimis transactions. In as much as the availability of cash is enhanced under the proposal, operators of retail stores are exempted from the requirement for a payment institution license when they offer cash withdrawal services without a purchase on their premises (on a voluntary basis), where the amount of cash distributed does not exceed EUR 50, in line with the need to avoid unfair competition with ATM deployers. Likewise benefitting from this exemption are distributors of cash via ATMs who do not service payment accounts – so-called

"independent ATM deployers" – and only have to fulfil a registration requirement which must be accompanied by certain documentation.

Focusing on FIDAR

As for the legislative proposal setting out a financial data access framework, the FIDAR proposal aims to establish clear rights and obligations allowing to manage the sharing of customer data in the financial sector beyond payment accounts notably to:

- mortgages, loans and accounts (other than payment accounts in scope of the PSR);
- savings products, financial instrument investments, crypto-assets, real estate and related investments;
- occupational and personal pension products;
- non-life insurance products (excluding sickness and health insurance); and
- data forming part of a creditworthiness assessment.

Consumer Right Act EU

DIRECTIVE 2011/83/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2011

On consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises (4) and Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (5) lay down a number of contractual rights for consumers.

(2) Those Directives have been reviewed in the light of experience with a view to simplifying and updating the applicable rules, removing inconsistencies and closing unwanted gaps in the rules. That review has shown that it is appropriate to replace those two Directives by a single Directive. This

Directive should therefore lay down standard rules for the common aspects of distance and off-premises contracts, moving away from the minimum harmonisation approach in the former Directives whilst allowing Member States to maintain or adopt national rules in relation to certain aspects.

(3) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through the measures adopted pursuant to Article 114 thereof.

(4) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured. The harmonisation of certain aspects of consumer distance and off-premises contracts is necessary for the promotion of a real consumer internal market striking the right balance between a high level of consumer protection and the competitiveness of enterprises, while ensuring respect for the principle of subsidiarity.

(5) The cross-border potential of distance selling, which should be one of the main tangible results of the internal market, is not fully exploited. Compared with the significant growth of domestic distance sales over the last few years, the growth in cross-border distance sales has been limited. This discrepancy is particularly significant for Internet sales for which the potential for further growth is high. The cross-border potential of contracts negotiated away from business premises (direct selling) is constrained by a number of factors including the different national consumer protection rules imposed upon the industry. Compared with the growth of domestic direct selling over the last few years, in particular in the services sector, for instance utilities, the number of consumers using this channel for cross-border purchases has remained flat. Responding to increased business opportunities in many Member States, small and medium-sized enterprises (including individual traders) or agents of direct selling companies should be more inclined to seek business opportunities in other Member States, in particular in border regions. Therefore the full harmonisation of consumer information and the right of withdrawal in distance and off-premises contracts will contribute to a high level of consumer protection and a better functioning of the business-to-consumer internal market.

(6) Certain disparities create significant internal market barriers affecting traders and consumers. Those disparities increase compliance costs to traders wishing to engage in the cross-border sale of goods or provision of services. Disproportionate fragmentation also undermines consumer confidence in the internal market.

(7) Full harmonisation of some key regulatory aspects should considerably increase legal certainty for both consumers and traders. Both consumers and traders should be able to rely on a single regulatory framework based on clearly defined legal concepts regulating certain aspects of business-to-consumer contracts across the Union. The effect of such harmonisation should be to eliminate the barriers stemming from the fragmentation of the rules and to complete the internal market in this area. Those barriers can only be eliminated by establishing uniform rules at Union level. Furthermore consumers should enjoy a high common level of protection across the Union.

(8) The regulatory aspects to be harmonised should only concern contracts concluded between traders and consumers. Therefore, this Directive should not affect national law in the area of contracts relating to employment, contracts relating to succession rights, contracts relating to family law and contracts relating to the incorporation and organisation of companies or partnership agreements.

(9) This Directive establishes rules on information to be provided for distance contracts, off-premises contracts and contracts other than distance and off-premises contracts. This Directive also regulates

the right of withdrawal for distance and off-premises contracts and harmonises certain provisions dealing with the performance and some other aspects of business-to-consumer contracts.

(10) This Directive should be without prejudice to Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (6).

(11) This Directive should be without prejudice to Union provisions relating to specific sectors, such as medicinal products for human use, medical devices, privacy and electronic communications, patients' rights in cross-border healthcare, food labelling and the internal market for electricity and natural gas.

(12) The information requirements provided for in this Directive should complete the information requirements of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (7) and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (8). Member States should retain the possibility to impose additional information requirements applicable to service providers established in their territory.

(13) Member States should remain competent, in accordance with Union law, to apply the provisions of this Directive to areas not falling within its scope. Member States may therefore maintain or introduce national legislation corresponding to the provisions of this Directive, or certain of its provisions, in relation to contracts that fall outside the scope of this Directive. For instance, Member States may decide to extend the application of the rules of this Directive to legal persons or to natural persons who are not consumers within the meaning of this Directive, such as non-governmental organisations, start-ups or small and medium-sized enterprises. Similarly, Member States may apply the provisions of this Directive to contracts that are not distance contracts within the meaning of this Directive, for example because they are not concluded under an organised distance sales or service-provision scheme. Moreover, Member States may also maintain or introduce national provisions on issues not specifically addressed in this Directive, such as additional rules concerning sales contracts, including in relation to the delivery of goods, or requirements for the provision of information during the existence of a contract.

(14) This Directive should not affect national law in the area of contract law for contract law aspects that are not regulated by this Directive. Therefore, this Directive should be without prejudice to national law regulating for instance the conclusion or the validity of a contract (for instance in the case of lack of consent). Similarly, this Directive should not affect national law in relation to the general contractual legal remedies, the rules on public economic order, for instance rules on excessive or extortionate prices, and the rules on unethical legal transactions.

(15) This Directive should not harmonise language requirements applicable to consumer contracts. Therefore, Member States may maintain or introduce in their national law language requirements regarding contractual information and contractual terms.

(16) This Directive should not affect national laws on legal representation such as the rules relating to the person who is acting in the name of the trader or on his behalf (such as an agent or a trustee). Member States should remain competent in this area. This Directive should apply to all traders, whether public or private.

(17) The definition of consumer should cover natural persons who are acting outside their trade, business, craft or profession. However, in the case of dual purpose contracts, where the contract is

concluded for purposes partly within and partly outside the person's trade and the trade purpose is so limited as not to be predominant in the overall context of the contract, that person should also be considered as a consumer.

(18) This Directive does not affect the freedom of Member States to define, in conformity with Union law, what they consider to be services of general economic interest, how those services should be organised and financed, in compliance with State aid rules, and which specific obligations they should be subject to.

(19) Digital content means data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means. Contracts for the supply of digital content should fall within the scope of this Directive. If digital content is supplied on a tangible medium, such as a CD or a DVD, it should be considered as goods within the meaning of this Directive. Similarly to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, contracts for digital content which is not supplied on a tangible medium should be classified, for the purpose of this Directive, neither as sales contracts nor as service contracts. For such contracts, the consumer should have a right of withdrawal unless he has consented to the beginning of the performance of the contract during the withdrawal period and has acknowledged that he will consequently lose the right to withdraw from the contract. In addition to the general information requirements, the trader should inform the consumer about the functionality and the relevant interoperability of digital content. The notion of functionality should refer to the ways in which digital content can be used, for instance for the tracking of consumer behaviour; it should also refer to the absence or presence of any technical restrictions such as protection via Digital Rights Management or region coding. The notion of relevant interoperability is meant to describe the information regarding the standard hardware and software environment with which the digital content is compatible, for instance the operating system, the necessary version and certain hardware features. The Commission should examine the need for further harmonisation of provisions in respect of digital content and submit, if necessary, a legislative proposal for addressing this matter.

(20) The definition of distance contract should cover all cases where a contract is concluded between the trader and the consumer under an organised distance sales or service-provision scheme, with the exclusive use of one or more means of distance communication (such as mail order, Internet, telephone or fax) up to and including the time at which the contract is concluded. That definition should also cover situations where the consumer visits the business premises merely for the purpose of gathering information about the goods or services and subsequently negotiates and concludes the contract at a distance. By contrast, a contract which is negotiated at the business premises of the trader and finally concluded by means of distance communication should not be considered a distance contract. Neither should a contract initiated by means of distance communication, but finally concluded at the business premises of the trader be considered a distance contract. Similarly, the concept of distance contract should not include reservations made by a consumer through a means of distance communications to request the provision of a service from a professional, such as in the case of a consumer phoning to request an appointment with a hairdresser. The notion of an organised distance sales or service-provision scheme should include those schemes offered by a third party other than the trader but used by the trader, such as an online platform. It should not, however, cover cases where websites merely offer information on the trader, his goods and/or services and his contact details.

(21) An off-premises contract should be defined as a contract concluded with the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader, for example at the consumer's home or workplace. In an off-premises context, the consumer may be under potential psychological pressure or may be confronted with an element of surprise, irrespective of whether or not the consumer has solicited the trader's visit. The definition of an off-premises contract should also include situations where the consumer is personally and individually addressed in an off-premises context but the contract is concluded immediately afterwards on the business premises of the trader or through a means of distance communication. The definition of an off-premises contract should not cover situations in which the trader first comes to the consumer's home strictly with a view to taking measurements or giving an estimate without any commitment of the consumer and where the contract is then concluded only at a later point in time on the business premises of the trader or via means of distance communication on the basis of the trader's estimate. In those cases, the contract is not to be considered as having been concluded immediately after the trader has addressed the consumer if the consumer has had time to reflect upon the estimate of the trader before concluding the contract. Purchases made during an excursion organised by the trader during which the products acquired are promoted and offered for sale should be considered as off-premises contracts.

(22) Business premises should include premises in whatever form (such as shops, stalls or lorries) which serve as a permanent or usual place of business for the trader. Market stalls and fair stands should be treated as business premises if they fulfil this condition. Retail premises where the trader carries out his activity on a seasonal basis, for instance during the tourist season at a ski or beach resort, should be considered as business premises as the trader carries out his activity in those premises on a usual basis. Spaces accessible to the public, such as streets, shopping malls, beaches, sports facilities and public transport, which the trader uses on an exceptional basis for his business activities as well as private homes or workplaces should not be regarded as business premises. The business premises of a person acting in the name or on behalf of the trader as defined in this Directive should be considered as business premises within the meaning of this Directive.

(23) Durable media should enable the consumer to store the information for as long as it is necessary for him to protect his interests stemming from his relationship with the trader. Such media should include in particular paper, USB sticks, CD-ROMs, DVDs, memory cards or the hard disks of computers as well as e-mails.

(24) A public auction implies that traders and consumers attend or are given the possibility to attend the auction in person. The goods or services are offered by the trader to the consumer through a bidding procedure authorised by law in some Member States, to offer goods or services at public sale. The successful bidder is bound to purchase the goods or services. The use of online platforms for auction purposes which are at the disposal of consumers and traders should not be considered as a public auction within the meaning of this Directive.

(25) Contracts related to district heating should be covered by this Directive, similarly to the contracts for the supply of water, gas or electricity. District heating refers to the supply of heat, inter alia, in the form of steam or hot water, from a central source of production through a transmission and distribution system to multiple buildings, for the purpose of heating.

(26) Contracts related to the transfer of immovable property or of rights in immovable property or to the creation or acquisition of such immovable property or rights, contracts for the construction of new buildings or the substantial conversion of existing buildings as well as contracts for the rental of accommodation for residential purposes are already subject to a number of specific requirements in national legislation. Those contracts include for instance sales of immovable property still to be developed and hire-purchase. The provisions of this Directive are not appropriate to those contracts,

which should be therefore excluded from its scope. A substantial conversion is a conversion comparable to the construction of a new building, for example where only the façade of an old building is retained. Service contracts in particular those related to the construction of annexes to buildings (for example a garage or a veranda) and those related to repair and renovation of buildings other than substantial conversion, should be included in the scope of this Directive, as well as contracts related to the services of a real estate agent and those related to the rental of accommodation for non-residential purposes.

(27) Transport services cover passenger transport and transport of goods. Passenger transport should be excluded from the scope of this Directive as it is already subject to other Union legislation or, in the case of public transport and taxis, to regulation at national level. However, the provisions of this Directive protecting consumers against excessive fees for the use of means of payment or against hidden costs should apply also to passenger transport contracts. In relation to transport of goods and car rental which are services, consumers should benefit from the protection afforded by this Directive, with the exception of the right of withdrawal.

(28) In order to avoid administrative burden being placed on traders, Member States may decide not to apply this Directive where goods or services of a minor value are sold off-premises. The monetary threshold should be established at a sufficiently low level as to exclude only purchases of small significance. Member States should be allowed to define this value in their national legislation provided that it does not exceed EUR 50. Where two or more contracts with related subjects are concluded at the same time by the consumer, the total cost thereof should be taken into account for the purpose of applying this threshold.

(29) Social services have fundamentally distinct features that are reflected in sector-specific legislation, partially at Union level and partially at national level. Social services include, on the one hand, services for particularly disadvantaged or low income persons as well as services for persons and families in need of assistance in carrying out routine, everyday tasks and, on the other hand, services for all people who have a special need for assistance, support, protection or encouragement in a specific life phase. Social services cover, inter alia, services for children and youth, assistance services for families, single parents and older persons, and services for migrants. Social services cover both short-term and long-term care services, for instance services provided by home care services or provided in assisted living facilities and residential homes or housing (‘nursing homes’). Social services include not only those provided by the State at a national, regional or local level by providers mandated by the State or by charities recognised by the State but also those provided by private operators. The provisions of this Directive are not appropriate to social services which should be therefore excluded from its scope.

(30) Healthcare requires special regulations because of its technical complexity, its importance as a service of general interest as well as its extensive public funding. Healthcare is defined in Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare (9) as ‘health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices’. Health professional is defined in that Directive as a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (10) or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in point (a) of Article 3(1) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment. The provisions of this Directive are not appropriate to healthcare which should be therefore excluded from its scope.

(31) Gambling should be excluded from the scope of this Directive. Gambling activities are those which involve wagering at stake with pecuniary value in games of chance, including lotteries, gambling in casinos and betting transactions. Member States should be able to adopt other, including more stringent, consumer protection measures in relation to such activities.

(32) The existing Union legislation, inter alia, relating to consumer financial services, package travel and timeshare contains numerous rules on consumer protection. For this reason, this Directive should not apply to contracts in those areas. With regard to financial services, Member States should be encouraged to draw inspiration from existing Union legislation in that area when legislating in areas not regulated at Union level, in such a way that a level playing field for all consumers and all contracts relating to financial services is ensured.

(33) The trader should be obliged to inform the consumer in advance of any arrangement resulting in the consumer paying a deposit to the trader, including an arrangement whereby an amount is blocked on the consumer's credit or debit card.

(34) The trader should give the consumer clear and comprehensible information before the consumer is bound by a distance or off-premises contract, a contract other than a distance or an off-premises contract, or any corresponding offer. In providing that information, the trader should take into account the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee. However, taking into account such specific needs should not lead to different levels of consumer protection.

(35) The information to be provided by the trader to the consumer should be mandatory and should not be altered. Nevertheless, the contracting parties should be able to expressly agree to change the content of the contract subsequently concluded, for instance the arrangements for delivery.

(36)In the case of distance contracts, the information requirements should be adapted to take into account the technical constraints of certain media, such as the restrictions on the number of characters on certain mobile telephone screens or the time constraint on television sales spots. In such cases the trader should comply with a minimum set of information requirements and refer the consumer to another source of information, for instance by providing a toll free telephone number or a hypertext link to a webpage of the trader where the relevant information is directly available and easily accessible. As to the requirement to inform the consumer of the cost of returning goods which by their nature cannot normally be returned by post, it will be considered to have been met, for example, if the trader specifies one carrier (for instance the one he assigned for the delivery of the good) and one price concerning the cost of returning the goods. Where the cost of returning the goods cannot reasonably be calculated in advance by the trader, for example because the trader does not offer to arrange for the return of the goods himself, the trader should provide a statement that such a cost will be payable, and that this cost may be high, along with a reasonable estimation of the maximum cost, which could be based on the cost of delivery to the consumer.

(37) Since in the case of distance sales, the consumer is not able to see the goods before concluding the contract, he should have a right of withdrawal. For the same reason, the consumer should be allowed to test and inspect the goods he has bought to the extent necessary to establish the nature, characteristics and the functioning of the goods. Concerning off-premises contracts, the consumer should have the right of withdrawal because of the potential surprise element and/or psychological pressure. Withdrawal from the contract should terminate the obligation of the contracting parties to perform the contract.

(38) Trading websites should indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

(39) It is important to ensure for distance contracts concluded through websites that the consumer is able to fully read and understand the main elements of the contract before placing his order. To that end, provision should be made in this Directive for those elements to be displayed in the close vicinity of the confirmation requested for placing the order. It is also important to ensure that, in such situations, the consumer is able to determine the moment at which he assumes the obligation to pay the trader. Therefore, the consumer's attention should specifically be drawn, through an unambiguous formulation, to the fact that placing the order entails the obligation to pay the trader.

(40) The current varying lengths of the withdrawal periods both between the Member States and for distance and off-premises contracts cause legal uncertainty and compliance costs. The same withdrawal period should apply to all distance and off-premises contracts. In the case of service contracts, the withdrawal period should expire after 14 days from the conclusion of the contract. In the case of sales contracts, the withdrawal period should expire after 14 days from the day on which the consumer or a third party other than the carrier and indicated by the consumer, acquires physical possession of the goods. In addition the consumer should be able to exercise the right to withdraw before acquiring physical possession of the goods. Where multiple goods are ordered by the consumer in one order but are delivered separately, the withdrawal period should expire after 14 days from the day on which the consumer acquires physical possession of the last good. Where goods are delivered in multiple lots or pieces, the withdrawal period should expire after 14 days from the day on which the consumer acquires the physical possession of the last lot or piece.

(41) In order to ensure legal certainty, it is appropriate that Council Regulation (EEC, Euratom) No 1182/71 of 3 June 1971 determining the rules applicable to periods, dates and time limits (11) should apply to the calculation of the periods contained in this Directive. Therefore, all periods contained in this Directive should be understood to be expressed in calendar days. Where a period expressed in days is to be calculated from the moment at which an event occurs or an action takes place, the day during which that event occurs or that action takes place should not be considered as falling within the period in question.

(42) The provisions relating to the right of withdrawal should be without prejudice to the Member States' laws and regulations governing the termination or unenforceability of a contract or the possibility for the consumer to fulfil his contractual obligations before the time determined in the contract.

(43) If the trader has not adequately informed the consumer prior to the conclusion of a distance or off-premises contract, the withdrawal period should be extended. However, in order to ensure legal certainty as regards the length of the withdrawal period, a 12-month limitation period should be introduced.

(44) Differences in the ways in which the right of withdrawal is exercised in the Member States have caused costs for traders selling cross-border. The introduction of a harmonised model withdrawal form that the consumer may use should simplify the withdrawal process and bring legal certainty. For these reasons, Member States should refrain from adding any presentational requirements to the Union-wide model form relating for example to the font size. However, the consumer should remain free to withdraw in his own words, provided that his statement setting out his decision to withdraw from the contract to the trader is unequivocal. A letter, a telephone call or returning the goods with a clear statement could meet this requirement, but the burden of proof of having withdrawn within the time limits fixed in the Directive should be on the consumer. For this reason, it is in the interest of the consumer to make use of a durable medium when communicating his withdrawal to the trader.

(45) As experience shows that many consumers and traders prefer to communicate via the trader's website, there should be a possibility for the trader to give the consumer the option of filling in a web-based withdrawal form. In this case the trader should provide an acknowledgement of receipt for instance by e-mail without delay.

(46) In the event that the consumer withdraws from the contract, the trader should reimburse all payments received from the consumer, including those covering the expenses borne by the trader to deliver goods to the consumer. The reimbursement should not be made by voucher unless the consumer has used vouchers for the initial transaction or has expressly accepted them. If the consumer expressly chooses a certain type of delivery (for instance 24-hour express delivery), although the trader had offered a common and generally acceptable type of delivery which would have incurred lower delivery costs, the consumer should bear the difference in costs between these two types of delivery.

(47) Some consumers exercise their right of withdrawal after having used the goods to an extent more than necessary to establish the nature, characteristics and the functioning of the goods. In this case the consumer should not lose the right to withdraw but should be liable for any diminished value of the goods. In order to establish the nature, characteristics and functioning of the goods, the consumer should only handle and inspect them in the same manner as he would be allowed to do in a shop. For example, the consumer should only try on a garment and should not be allowed to wear it. Consequently, the consumer should handle and inspect the goods with due care during the withdrawal period. The obligations of the consumer in the event of withdrawal should not discourage the consumer from exercising his right of withdrawal.

(48) The consumer should be required to send back the goods not later than 14 days after having informed the trader about his decision to withdraw from the contract. In situations where the trader or the consumer does not fulfil the obligations relating to the exercise of the right of withdrawal, penalties provided for by national legislation in accordance with this Directive should apply as well as contract law provisions.

(49) Certain exceptions from the right of withdrawal should exist, both for distance and off-premises contracts. A right of withdrawal could be inappropriate for example given the nature of particular goods or services. That is the case for example with wine supplied a long time after the conclusion of a contract of a speculative nature where the value is dependent on fluctuations in the market ('vin en primeur'). The right of withdrawal should neither apply to goods made to the consumer's specifications or which are clearly personalised such as tailor-made curtains, nor to the supply of fuel, for example, which is a good, by nature inseparably mixed with other items after delivery. The granting of a right of withdrawal to the consumer could also be inappropriate in the case of certain services where the conclusion of the contract implies the setting aside of capacity which, if a right of withdrawal were exercised, the trader may find difficult to fill. This would for example be the case where reservations are made at hotels or concerning holiday cottages or cultural or sporting events.

(50) On the one hand, the consumer should benefit from his right of withdrawal even in case he has asked for the provision of services before the end of the withdrawal period. On the other hand, if the consumer exercises his right of withdrawal, the trader should be assured to be adequately paid for the service he has provided. The calculation of the proportionate amount should be based on the price agreed in the contract unless the consumer demonstrates that that total price is itself disproportionate, in which case the amount to be paid shall be calculated on the basis of the market value of the service provided. The market value should be defined by comparing the price of an equivalent service performed by other traders at the time of the conclusion of the contract. Therefore the consumer

should request the performance of services before the end of the withdrawal period by making this request expressly and, in the case of off-premises contracts, on a durable medium. Similarly, the trader should inform the consumer on a durable medium of any obligation to pay the proportionate costs for the services already provided. For contracts having as their object both goods and services, the rules provided for in this Directive on the return of goods should apply to the goods aspects and the compensation regime for services should apply to the services aspects.

(51) The main difficulties encountered by consumers and one of the main sources of disputes with traders concern delivery of goods, including goods getting lost or damaged during transport and late or partial delivery. Therefore it is appropriate to clarify and harmonise the national rules as to when delivery should occur. The place and modalities of delivery and the rules concerning the determination of the conditions for the transfer of the ownership of the goods and the moment at which such transfer takes place, should remain subject to national law and therefore should not be affected by this Directive. The rules on delivery laid down in this Directive should include the possibility for the consumer to allow a third party to acquire on his behalf the physical possession or control of the goods. The consumer should be considered to have control of the goods where he or a third party indicated by the consumer has access to the goods to use them as an owner, or the ability to resell the goods (for example, when he has received the keys or possession of the ownership documents).

(52) In the context of sales contracts, the delivery of goods can take place in various ways, either immediately or at a later date. If the parties have not agreed on a specific delivery date, the trader should deliver the goods as soon as possible, but in any event not later than 30 days from the day of the conclusion of the contract. The rules regarding late delivery should also take into account goods to be manufactured or acquired specially for the consumer which cannot be reused by the trader without considerable loss. Therefore, a rule which grants an additional reasonable period of time to the trader in certain circumstances should be provided for in this Directive. When the trader has failed to deliver the goods within the period of time agreed with the consumer, before the consumer can terminate the contract, the consumer should call upon the trader to make the delivery within a reasonable additional period of time and be entitled to terminate the contract if the trader fails to deliver the goods even within that additional period of time. However, this rule should not apply when the trader has refused to deliver the goods in an unequivocal statement. Neither should it apply in certain circumstances where the delivery period is essential such as, for example, in the case of a wedding dress which should be delivered before the wedding. Nor should it apply in circumstances where the consumer informs the trader that delivery on a specified date is essential. For this purpose, the consumer may use the trader’s contact details given in accordance with this Directive. In these specific cases, if the trader fails to deliver the goods on time, the consumer should be entitled to terminate the contract immediately after the expiry of the delivery period initially agreed. This Directive should be without prejudice to national provisions on the way the consumer should notify the trader of his will to terminate the contract.

(53) In addition to the consumer’s right to terminate the contract where the trader has failed to fulfil his obligations to deliver the goods in accordance with this Directive, the consumer may, in accordance with the applicable national law, have recourse to other remedies, such as granting the trader an additional period of time for delivery, enforcing the performance of the contract, withholding payment, and seeking damages.

(54) In accordance with Article 52(3) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (12), Member States should be able to prohibit or limit traders’ right to request charges from consumers taking into account the need to encourage competition and promote the use of efficient payment instruments. In any event,

traders should be prohibited from charging consumers fees that exceed the cost borne by the trader for the use of a certain means of payment.

(55) Where the goods are dispatched by the trader to the consumer, disputes may arise, in the event of loss or damage, as to the moment at which the transfer of risk takes place. Therefore this Directive should provide that the consumer be protected against any risk of loss of or damage to the goods occurring before he has acquired the physical possession of the goods. The consumer should be protected during a transport arranged or carried out by the trader, even where the consumer has chosen a particular delivery method from a range of options offered by the trader. However, that provision should not apply to contracts where it is up to the consumer to take delivery of the goods himself or to ask a carrier to take delivery. Regarding the moment of the transfer of the risk, a consumer should be considered to have acquired the physical possession of the goods when he has received them.

(56) Persons or organisations regarded under national law as having a legitimate interest in protecting consumer contractual rights should be afforded the right to initiate proceedings, either before a court or before an administrative authority which is competent to decide upon complaints or to initiate appropriate legal proceedings.

(57) It is necessary that Member States lay down penalties for infringements of this Directive and ensure that they are enforced. The penalties should be effective, proportionate and dissuasive.

(58) The consumer should not be deprived of the protection granted by this Directive. Where the law applicable to the contract is that of a third country, Regulation (EC) No 593/2008 should apply, in order to determine whether the consumer retains the protection granted by this Directive.

(59) The Commission, following consultation with the Member States and stakeholders, should look into the most appropriate way to ensure that all consumers are made aware of their rights at the point of sale.

(60) Since inertia selling, which consists of unsolicited supply of goods or provision of services to consumers, is prohibited by Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (‘Unfair Commercial Practices Directive’) (13) but no contractual remedy is provided therein, it is necessary to introduce in this Directive the contractual remedy of exempting the consumer from the obligation to provide any consideration for such unsolicited supply or provision.

(61) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (14) already regulates unsolicited communications and provides for a high level of consumer protection. The corresponding provisions on the same issue contained in Directive 97/7/EC are therefore not needed.

(62) It is appropriate for the Commission to review this Directive if some barriers to the internal market are identified. In its review, the Commission should pay particular attention to the possibilities granted to Member States to maintain or introduce specific national provisions including in certain areas of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (15) and Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees (16). That review could lead to a Commission proposal to amend this Directive; that proposal may include amendments to other

consumer protection legislation reflecting the Commission's Consumer Policy Strategy commitment to review the Union acquis in order to achieve a high, common level of consumer protection.

(63) Directives 93/13/EEC and 1999/44/EC should be amended to require Member States to inform the Commission about the adoption of specific national provisions in certain areas.

(64) Directives 85/577/EEC and 97/7/EC should be repealed.

(65) Since the objective of this Directive, namely, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(66) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

(67) In accordance with point 34 of the Interinstitutional agreement on better law-making (17), Member States are encouraged to draw up, for themselves and in the interests of the Union, their own tables, which will, as far as possible, illustrate the correlation between this Directive and the transposition measures, and to make them public,

3.7 Consumer protection Act [9]

The Consumer Rights Directive 2011/83/EU[1] is a consumer protection measure in EU law.[2][3] It was due to be implemented by 13 December 2013. The Directive applies to most contracts between traders and consumers and applied to all contracts concluded after 13 June 2014.[6] Exceptions include financial services, gambling, healthcare by regulated professionals, package travel,[7] property transactions, social services, timeshare[7] and most aspects of passenger transport.

CHAPTER I

SUBJECT MATTER, DEFINITIONS AND SCOPE

Article 1

Subject matter

The purpose of this Directive is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market by approximating certain aspects of the laws, regulations and administrative provisions of the Member States concerning contracts concluded between consumers and traders.

Article 2

Definitions

For the purpose of this Directive, the following definitions shall apply:

(1) ‘consumer’ means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession;

(2) ‘trader’ means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive;

(3) ‘goods’ means any tangible movable items, with the exception of items sold by way of execution or otherwise by authority of law; water, gas and electricity shall be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity;

(4) ‘goods made to the consumer’s specifications’ means non-prefabricated goods made on the basis of an individual choice of or decision by the consumer;

(5) ‘sales contract’ means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price thereof, including any contract having as its object both goods and services;

(6) ‘service contract’ means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof;

(7) ‘distance contract’ means any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded;

(8) ‘off-premises contract’ means any contract between the trader and the consumer:

a. concluded in the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader;

b. for which an offer was made by the consumer in the same circumstances as referred to in point (a);

c. concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader in the simultaneous physical presence of the trader and the consumer; or

d. concluded during an excursion organised by the trader with the aim or effect of promoting and selling goods or services to the consumer;

(9) ‘business premises’ means:

a. any immovable retail premises where the trader carries out his activity on a permanent basis; or

b. any movable retail premises where the trader carries out his activity on a usual basis;

(10) ‘durable medium’ means any instrument which enables the consumer or the trader to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored;

(11) ‘digital content’ means data which are produced and supplied in digital form;

(12) ‘financial service’ means any service of a banking, credit, insurance, personal pension, investment or payment nature;

(13) ‘public auction’ means a method of sale where goods or services are offered by the trader to consumers, who attend or are given the possibility to attend the auction in person, through a transparent, competitive bidding procedure run by an auctioneer and where the successful bidder is bound to purchase the goods or services.

(14) ‘commercial guarantee’ means any undertaking by the trader or a producer (the guarantor) to the consumer, in addition to his legal obligation relating to the guarantee of conformity, to reimburse the price paid or to replace, repair or service goods in any way if they do not meet the specifications or any other requirements not related to conformity set out in the guarantee statement or in the relevant advertising available at the time of, or before the conclusion of the contract;

(15) ‘ancillary contract’ means a contract by which the consumer acquires goods or services related to a distance contract or an off-premises contract and where those goods are supplied or those services are provided by the trader or by a third party on the basis of an arrangement between that third party and the trader.

Article 3

Scope

1. This Directive shall apply, under the conditions and to the extent set out in its provisions, to any contract concluded between a trader and a consumer. It shall also apply to contracts for the supply of water, gas, electricity or district heating, including by public providers, to the extent that these commodities are provided on a contractual basis.

2. If any provision of this Directive conflicts with a provision of another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

3. This Directive shall not apply to contracts:

(a) for social services, including social housing, childcare and support of families and persons permanently or temporarily in need, including long-term care;

(b) for healthcare as defined in point (a) of Article 3 of Directive 2011/24/EU, whether or not they are provided via healthcare facilities;

(c) for gambling, which involves wagering a stake with pecuniary value in games of chance, including lotteries, casino games and betting transactions;

(d)for financial services;

(e) for the creation, acquisition or transfer of immovable property or of rights in immovable property;

(f) for the construction of new buildings, the substantial conversion of existing buildings and for rental of accommodation for residential purposes;

(g) which fall within the scope of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours (18);

(h) which fall within the scope of Directive 2008/122/EC of the European Parliament and of the Council of 14 January 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts (19);

(i) which, in accordance with the laws of Member States, are established by a public office-holder who has a statutory obligation to be independent and impartial and who must ensure, by providing comprehensive legal information, that the consumer only concludes the contract on the basis of careful legal consideration and with knowledge of its legal scope;

(j) for the supply of foodstuffs, beverages or other goods intended for current consumption in the household, and which are physically supplied by a trader on frequent and regular rounds to the consumer's home, residence or workplace;

(k) for passenger transport services, with the exception of Article 8(2) and Articles 19 and 22;

(l) concluded by means of automatic vending machines or automated commercial premises;

(m) concluded with telecommunications operators through public payphones for their use or concluded for the use of one single connection by telephone, Internet or fax established by a consumer.

4. Member States may decide not to apply this Directive or not to maintain or introduce corresponding national provisions to off-premises contracts for which the payment to be made by the consumer does not exceed EUR 50. Member States may define a lower value in their national legislation.

5. This Directive shall not affect national general contract law such as the rules on the validity, formation or effect of a contract, in so far as general contract law aspects are not regulated in this Directive.

6. This Directive shall not prevent traders from offering consumers contractual arrangements which go beyond the protection provided for in this Directive.

Article 4

Level of harmonisation

Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more or less stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive.

CHAPTER II

CONSUMER INFORMATION FOR CONTRACTS OTHER THAN DISTANCE OR OFF-PREMISES CONTRACTS

Article 5

Information requirements for contracts other than distance or off-premises contracts

1. Before the consumer is bound by a contract other than a distance or an off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner, if that information is not already apparent from the context:

(a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;

(b) the identity of the trader, such as his trading name, the geographical address at which he is established and his telephone number;

(c) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable;

(d) where applicable, the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the service, and the trader’s complaint handling policy;

(e) in addition to a reminder of the existence of a legal guarantee of conformity for goods, the existence and the conditions of after-sales services and commercial guarantees, where applicable;

(f) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(g) where applicable, the functionality, including applicable technical protection measures, of digital content;

(h) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. Member States shall not be required to apply paragraph 1 to contracts which involve day-to-day transactions and which are performed immediately at the time of their conclusion.

4. Member States may adopt or maintain additional pre-contractual information requirements for contracts to which this Article applies.

CHAPTER III

CONSUMER INFORMATION AND RIGHT OF WITHDRAWAL FOR DISTANCE AND OFF-PREMISES CONTRACTS

Article 6

Information requirements for distance and off-premises contracts

1. Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner:

(a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;

(b) the identity of the trader, such as his trading name;

(c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;

(d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;

(e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;

(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11(1), as well as the model withdrawal form set out in Annex I(B);

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;

(j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14(3);

(k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;

(l) a reminder of the existence of a legal guarantee of conformity for goods;

(m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;

(n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable;

(o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(p) where applicable, the minimum duration of the consumer's obligations under the contract;

(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;

(r) where applicable, the functionality, including applicable technical protection measures, of digital content;

(s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of;

(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

2. Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.

3. In the case of a public auction, the information referred to in points (b), (c) and (d) of paragraph 1 may be replaced by the equivalent details for the auctioneer.

4. The information referred to in points (h), (i) and (j) of paragraph 1 may be provided by means of the model instructions on withdrawal set out in Annex I(A). The trader shall have fulfilled the information requirements laid down in points (h), (i) and (j) of paragraph 1 if he has supplied these instructions to the consumer, correctly filled in.

5. The information referred to in paragraph 1 shall form an integral part of the distance or off-premises contract and shall not be altered unless the contracting parties expressly agree otherwise.

6. If the trader has not complied with the information requirements on additional charges or other costs as referred to in point (e) of paragraph 1, or on the costs of returning the goods as referred to in point (i) of paragraph 1, the consumer shall not bear those charges or costs.

7. Member States may maintain or introduce in their national law language requirements regarding the contractual information, so as to ensure that such information is easily understood by the consumer.

8. The information requirements laid down in this Directive are in addition to information requirements contained in Directive 2006/123/EC and Directive 2000/31/EC and do not prevent Member States from imposing additional information requirements in accordance with those Directives.

Without prejudice to the first subparagraph, if a provision of Directive 2006/123/EC or Directive 2000/31/EC on the content and the manner in which the information is to be provided conflicts with a provision of this Directive, the provision of this Directive shall prevail.

9. As regards compliance with the information requirements laid down in this Chapter, the burden of proof shall be on the trader.

Article 7

Formal requirements for off-premises contracts

1. With respect to off-premises contracts, the trader shall give the information provided for in Article 6(1) to the consumer on paper or, if the consumer agrees, on another durable medium. That information shall be legible and in plain, intelligible language.

2. The trader shall provide the consumer with a copy of the signed contract or the confirmation of the contract on paper or, if the consumer agrees, on another durable medium, including, where applicable, the confirmation of the consumer's prior express consent and acknowledgement in accordance with point (m) of Article 16.

3. Where a consumer wants the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer makes such an express request on a durable medium.

4. With respect to off-premises contracts where the consumer has explicitly requested the services of the trader for the purpose of carrying out repairs or maintenance for which the trader and the consumer immediately perform their contractual obligations and where the payment to be made by the consumer does not exceed EUR 200:

(a) the trader shall provide the consumer with the information referred to in points (b) and (c) of Article 6(1) and information about the price or the manner in which the price is to be calculated together with an estimate of the total price, on paper or, if the consumer agrees, on another durable medium. The trader shall provide the information referred to in points (a), (h) and (k) of Article 6(1), but may choose not to provide it on paper or another durable medium if the consumer expressly agrees;

(b) the confirmation of the contract provided in accordance with paragraph 2 of this Article shall contain the information provided for in Article 6(1).

Member States may decide not to apply this paragraph.

5. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 8

Formal requirements for distance contracts

1. With respect to distance contracts, the trader shall give the information provided for in Article 6(1) or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible.

2. If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1).

The trader shall ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. If placing an order entails activating a button or a similar function, the button or similar function shall be labelled in an easily legible manner only with the words ‘order with obligation to pay’ or a corresponding unambiguous formulation indicating that placing the order entails an obligation to pay the trader. If the trader has not complied with this subparagraph, the consumer shall not be bound by the contract or order.

3. Trading websites shall indicate clearly and legibly at the latest at the beginning of the ordering process whether any delivery restrictions apply and which means of payment are accepted.

4. If the contract is concluded through a means of distance communication which allows limited space or time to display the information, the trader shall provide, on that particular means prior to the conclusion of such a contract, at least the pre-contractual information regarding the main characteristics of the goods or services, the identity of the trader, the total price, the right of withdrawal, the duration of the contract and, if the contract is of indeterminate duration, the conditions for terminating the contract, as referred to in points (a), (b), (e), (h) and (o) of Article 6(1). The other information referred to in Article 6(1) shall be provided by the trader to the consumer in an appropriate way in accordance with paragraph 1 of this Article.

5. Without prejudice to paragraph 4, if the trader makes a telephone call to the consumer with a view to concluding a distance contract, he shall, at the beginning of the conversation with the consumer, disclose his identity and, where applicable, the identity of the person on whose behalf he makes that call, and the commercial purpose of the call.

6. Where a distance contract is to be concluded by telephone, Member States may provide that the trader has to confirm the offer to the consumer who is bound only once he has signed the offer or has sent his written consent. Member States may also provide that such confirmations have to be made on a durable medium.

7. The trader shall provide the consumer with the confirmation of the contract concluded, on a durable medium within a reasonable time after the conclusion of the distance contract, and at the latest at the time of the delivery of the goods or before the performance of the service begins. That confirmation shall include:

(a) all the information referred to in Article 6(1) unless the trader has already provided that information to the consumer on a durable medium prior to the conclusion of the distance contract; and

(b) where applicable, the confirmation of the consumer's prior express consent and acknowledgment in accordance with point (m) of Article 16.

8. Where a consumer wants the performance of services, or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, to begin during the withdrawal period provided for in Article 9(2), the trader shall require that the consumer make an express request.

9. This Article shall be without prejudice to the provisions on the conclusion of e-contracts and the placing of e-orders set out in Articles 9 and 11 of Directive 2000/31/EC.

10. Member States shall not impose any further formal pre-contractual information requirements for the fulfilment of the information obligations laid down in this Directive.

Article 9

Right of withdrawal

1. Save where the exceptions provided for in Article 16 apply, the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14.

2. Without prejudice to Article 10, the withdrawal period referred to in paragraph 1 of this Article shall expire after 14 days from:

(a) in the case of service contracts, the day of the conclusion of the contract;

(b) in the case of sales contracts, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the goods or:

a) in the case of multiple goods ordered by the consumer in one order and delivered separately, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last good;

b) in the case of delivery of a good consisting of multiple lots or pieces, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the last lot or piece;

c) in the case of contracts for regular delivery of goods during defined period of time, the day on which the consumer or a third party other than the carrier and indicated by the consumer acquires physical possession of the first good;

(c) in the case of contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium, the day of the conclusion of the contract.

3. The Member States shall not prohibit the contracting parties from performing their contractual obligations during the withdrawal period. Nevertheless, in the case of off-premises contracts, Member States may maintain existing national legislation prohibiting the trader from collecting the payment from the consumer during the given period after the conclusion of the contract.

Article 10

Omission of information on the right of withdrawal

1. If the trader has not provided the consumer with the information on the right of withdrawal as required by point (h) of Article 6(1), the withdrawal period shall expire 12 months from the end of the initial withdrawal period, as determined in accordance with Article 9(2).

2. If the trader has provided the consumer with the information provided for in paragraph 1 of this Article within 12 months from the day referred to in Article 9(2), the withdrawal period shall expire 14 days after the day upon which the consumer receives that information.

Article 11

Exercise of the right of withdrawal

1. Before the expiry of the withdrawal period, the consumer shall inform the trader of his decision to withdraw from the contract. For this purpose, the consumer may either:

(a) use the model withdrawal form as set out in Annex I(B); or

(b) make any other unequivocal statement setting out his decision to withdraw from the contract.

Member States shall not provide for any formal requirements applicable to the model withdrawal form other than those set out in Annex I(B).

2. The consumer shall have exercised his right of withdrawal within the withdrawal period referred to in Article 9(2) and Article 10 if the communication concerning the exercise of the right of withdrawal is sent by the consumer before that period has expired.

3. The trader may, in addition to the possibilities referred to in paragraph 1, give the option to the consumer to electronically fill in and submit either the model withdrawal form set out in Annex I(B) or any other unequivocal statement on the trader’s website. In those cases the trader shall communicate to the consumer an acknowledgement of receipt of such a withdrawal on a durable medium without delay.

4. The burden of proof of exercising the right of withdrawal in accordance with this Article shall be on the consumer.

Article 12

Effects of withdrawal

The exercise of the right of withdrawal shall terminate the obligations of the parties:

(a) to perform the distance or off-premises contract; or

(b) to conclude the distance or off-premises contract, in cases where an offer was made by the consumer.

Article 13

Obligations of the trader in the event of withdrawal

1. The trader shall reimburse all payments received from the consumer, including, if applicable, the costs of delivery without undue delay and in any event not later than 14 days from the day on which he is informed of the consumer's decision to withdraw from the contract in accordance with Article 11.

The trader shall carry out the reimbursement referred to in the first subparagraph using the same means of payment as the consumer used for the initial transaction, unless the consumer has expressly agreed otherwise and provided that the consumer does not incur any fees as a result of such reimbursement.

2. Notwithstanding paragraph 1, the trader shall not be required to reimburse the supplementary costs, if the consumer has expressly opted for a type of delivery other than the least expensive type of standard delivery offered by the trader.

3. Unless the trader has offered to collect the goods himself, with regard to sales contracts, the trader may withhold the reimbursement until he has received the goods back, or until the consumer has supplied evidence of having sent back the goods, whichever is the earliest.

Article 14

Obligations of the consumer in the event of withdrawal

1. Unless the trader has offered to collect the goods himself, the consumer shall send back the goods or hand them over to the trader or to a person authorised by the trader to receive the goods, without undue delay and in any event not later than 14 days from the day on which he has communicated his decision to withdraw from the contract to the trader in accordance with Article 11. The deadline shall be met if the consumer sends back the goods before the period of 14 days has expired.

The consumer shall only bear the direct cost of returning the goods unless the trader has agreed to bear them or the trader failed to inform the consumer that the consumer has to bear them.

In the case of off-premises contracts where the goods have been delivered to the consumer's home at the time of the conclusion of the contract, the trader shall at his own expense collect the goods if, by their nature, those goods cannot normally be returned by post.

2. The consumer shall only be liable for any diminished value of the goods resulting from the handling of the goods other than what is necessary to establish the nature, characteristics and functioning of the goods. The consumer shall in any event not be liable for diminished value of the goods where the trader has failed to provide notice of the right of withdrawal in accordance with point (h) of Article 6(1).

3. Where a consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall pay to the trader an amount which is in proportion to what has been provided until the time the consumer has informed the trader of the exercise of the right of withdrawal, in comparison with the full coverage of the contract. The proportionate amount to be paid by the consumer to the trader shall be calculated on the basis of the total price agreed in the contract. If the total price is excessive, the proportionate amount shall be calculated on the basis of the market value of what has been provided.

4. The consumer shall bear no cost for:

(a) the performance of services or the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, or of district heating, in full or in part, during the withdrawal period, where:

(i) the trader has failed to provide information in accordance with points (h) or (j) of Article 6(1); or

(ii) the consumer has not expressly requested performance to begin during the withdrawal period in accordance with Article 7(3) and Article 8(8); or

(b) the supply, in full or in part, of digital content which is not supplied on a tangible medium where:

(i) the consumer has not given his prior express consent to the beginning of the performance before the end of the 14-day period referred to in Article 9;

(ii) the consumer has not acknowledged that he loses his right of withdrawal when giving his consent; or

(iii) the trader has failed to provide confirmation in accordance with Article 7(2) or Article 8(7).

5. Except as provided for in Article 13(2) and in this Article, the consumer shall not incur any liability as a consequence of the exercise of the right of withdrawal.

Article 15

Effects of the exercise of the right of withdrawal on ancillary contracts

1. Without prejudice to Article 15 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers (20), if the consumer exercises his right of withdrawal from a distance or an off-premises contract in accordance with Articles 9 to 14 of this

Directive, any ancillary contracts shall be automatically terminated, without any costs for the consumer, except as provided for in Article 13(2) and in Article 14 of this Directive.

2. The Member States shall lay down detailed rules on the termination of such contracts.

Article 16

Exceptions from the right of withdrawal

Member States shall not provide for the right of withdrawal set out in Articles 9 to 15 in respect of distance and off-premises contracts as regards the following:

(a) service contracts after the service has been fully performed if the performance has begun with the consumer's prior express consent, and with the acknowledgement that he will lose his right of withdrawal once the contract has been fully performed by the trader;

(b) the supply of goods or services for which the price is dependent on fluctuations in the financial market which cannot be controlled by the trader and which may occur within the withdrawal period;

(c)the supply of goods made to the consumer's specifications or clearly personalised;

(d)the supply of goods which are liable to deteriorate or expire rapidly;

(e)the supply of sealed goods which are not suitable for return due to health protection or hygiene reasons and were unsealed after delivery;

(f)the supply of goods which are, after delivery, according to their nature, inseparably mixed with other items;

(g)the supply of alcoholic beverages, the price of which has been agreed upon at the time of the conclusion of the sales contract, the delivery of which can only take place after 30 days and the actual value of which is dependent on fluctuations in the market which cannot be controlled by the trader;

(h)contracts where the consumer has specifically requested a visit from the trader for the purpose of carrying out urgent repairs or maintenance. If, on the occasion of such visit, the trader provides services in addition to those specifically requested by the consumer or goods other than replacement parts necessarily used in carrying out the maintenance or in making the repairs, the right of withdrawal shall apply to those additional services or goods;

(i)the supply of sealed audio or sealed video recordings or sealed computer software which were unsealed after delivery;

(j)the supply of a newspaper, periodical or magazine with the exception of subscription contracts for the supply of such publications;

(k)contracts concluded at a public auction;

(l)the provision of accommodation other than for residential purpose, transport of goods, car rental services, catering or services related to leisure activities if the contract provides for a specific date or period of performance;

(m)the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal.

CHAPTER IV

OTHER CONSUMER RIGHTS

Article 17

Scope

1. Articles 18 and 20 shall apply to sales contracts. Those Articles shall not apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or the supply of digital content which is not supplied on a tangible medium.

2. Articles 19, 21 and 22 shall apply to sales and service contracts and to contracts for the supply of water, gas, electricity, district heating or digital content.

Article 18

Delivery

1. Unless the parties have agreed otherwise on the time of delivery, the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay, but not later than 30 days from the conclusion of the contract.

2. Where the trader has failed to fulfil his obligation to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall call upon him to make the delivery within an additional period of time appropriate to the circumstances. If the trader fails to deliver the goods within that additional period of time, the consumer shall be entitled to terminate the contract.

The first subparagraph shall not be applicable to sales contracts where the trader has refused to deliver the goods or where delivery within the agreed delivery period is essential taking into account all the circumstances attending the conclusion of the contract or where the consumer informs the trader, prior to the conclusion of the contract, that delivery by or on a specified date is essential. In those cases, if the trader fails to deliver the goods at the time agreed upon with the consumer or within the time limit set out in paragraph 1, the consumer shall be entitled to terminate the contract immediately.

3. Upon termination of the contract, the trader shall, without undue delay, reimburse all sums paid under the contract.

4. In addition to the termination of the contract in accordance with paragraph 2, the consumer may have recourse to other remedies provided for by national law.

Article 19

Fees for the use of means of payment

Member States shall prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such means.

Article 20

Passing of risk

In contracts where the trader dispatches the goods to the consumer, the risk of loss of or damage to the goods shall pass to the consumer when he or a third party indicated by the consumer and other than the carrier has acquired the physical possession of the goods. However, the risk shall pass to the consumer upon delivery to the carrier if the carrier was commissioned by the consumer to carry the goods and that choice was not offered by the trader, without prejudice to the rights of the consumer against the carrier.

Article 21

Communication by telephone

Member States shall ensure that where the trader operates a telephone line for the purpose of contacting him by telephone in relation to the contract concluded, the consumer, when contacting the trader is not bound to pay more than the basic rate.

The first subparagraph shall be without prejudice to the right of telecommunication services providers to charge for such calls.

Article 22

Additional payments

Before the consumer is bound by the contract or offer, the trader shall seek the express consent of the consumer to any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation. If the trader has not obtained the consumer's express consent but has inferred it by using default options which the consumer is required to reject in order to avoid the additional payment, the consumer shall be entitled to reimbursement of this payment.

CHAPTER V

GENERAL PROVISIONS

Article 23

Enforcement

1. Member States shall ensure that adequate and effective means exist to ensure compliance with this Directive.

2. The means referred to in paragraph 1 shall include provisions whereby one or more of the following bodies, as determined by national law, may take action under national law before the courts

or before the competent administrative bodies to ensure that the national provisions transposing this Directive are applied:

(a)public bodies or their representatives;

(b)consumer organisations having a legitimate interest in protecting consumers;

(c)professional organisations having a legitimate interest in acting.

Article 24

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

2. Member States shall notify those provisions to the Commission by 13 December 2013 and shall notify it without delay of any subsequent amendment affecting them.

Article 25

Imperative nature of the Directive

If the law applicable to the contract is the law of a Member State, consumers may not waive the rights conferred on them by the national measures transposing this Directive.

Any contractual terms which directly or indirectly waive or restrict the rights resulting from this Directive shall not be binding on the consumer.

Article 26

Information

Member States shall take appropriate measures to inform consumers and traders of the national provisions transposing this Directive and shall, where appropriate, encourage traders and code owners as defined in point (g) of Article 2 of Directive 2005/29/EC, to inform consumers of their codes of conduct.

Article 27

Inertia selling

The consumer shall be exempted from the obligation to provide any consideration in cases of unsolicited supply of goods, water, gas, electricity, district heating or digital content or unsolicited provision of services, prohibited by Article 5(5) and point 29 of Annex I to Directive 2005/29/EC. In such cases, the absence of a response from the consumer following such an unsolicited supply or provision shall not constitute consent.

Article 28

Transposition

1. Member States shall adopt and publish, by 13 December 2013, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of these measures in the form of documents. The Commission shall make use of these documents for the purposes of the report referred to in Article 30.

They shall apply those measures from 13 June 2014.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. The provisions of this Directive shall apply to contracts concluded after 13 June 2014.

Article 29

Reporting requirements

1. Where a Member State makes use of any of the regulatory choices referred to in Article 3(4), Article 6(7), Article 6(8), Article 7(4), Article 8(6) and Article 9(3), it shall inform the Commission thereof by 13 December 2013, as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.

Article 30

Reporting by the Commission and review

By 13 December 2016, the Commission shall submit a report on the application of this Directive to the European Parliament and the Council. That report shall include in particular an evaluation of the provisions of this Directive regarding digital content including the right of withdrawal. The report shall be accompanied, where necessary, by legislative proposals to adapt this Directive to developments in the field of consumer rights.

CHAPTER VI

FINAL PROVISIONS

Article 31

Repeals

Directive 85/577/EEC and Directive 97/7/EC, as amended by Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services (21) and by Directives 2005/29/EC and 2007/64/EC, are repealed as of 13 June 2014.

References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex II.

Article 32

Amendment to Directive 93/13/EEC

In Directive 93/13/EEC, the following Article is inserted:

‘Article 8a

1. Where a Member State adopts provisions in accordance with Article 8, it shall inform the Commission thereof, as well as of any subsequent changes, in particular where those provisions:

—extend the unfairness assessment to individually negotiated contractual terms or to the adequacy of the price or remuneration; or,

—contain lists of contractual terms which shall be considered as unfair,

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.’

Article 33

Amendment to Directive 1999/44/EC

In Directive 1999/44/EC, the following Article is inserted:

‘Article 8a

Reporting requirements

1. Where, in accordance with Article 8(2), a Member State adopts more stringent consumer protection provisions than those provided for in Article 5(1) to (3) and in Article 7(1), it shall inform the Commission thereof, as well as of any subsequent changes.

2. The Commission shall ensure that the information referred to in paragraph 1 is easily accessible to consumers and traders, inter alia, on a dedicated website.

3. The Commission shall forward the information referred to in paragraph 1 to the other Member States and the European Parliament. The Commission shall consult stakeholders on that information.’

Article 34

Entry into force

This Directive shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

Article 35

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 25 October 2011.

For the European Parliament

The President

J. BUZEK

For the Council

The President

M. DOWGIELEWICZ

4 Prototype of the Regulatory Farmework Online Tool addressing laws and regulations for FAME

In this section we provide a snapshot of Regulatory Framework Online Tool addressing laws and regulations for FAME. The tool is already operationalized with necessary information about background study on laws and regulations. The tool also encompasses an information services section which users can find information related to data protection for the financial sector. The tool also includes a short description on the FAME project, providing related information about the project. Recent news is listed as a subsection of the website wich provides update on regulatory ecosystem of FAME for different stakeholders. The tool provides EU data protection regulations which lists the most relevant policies and Regulatiosn on Data Protection and Data Governance.

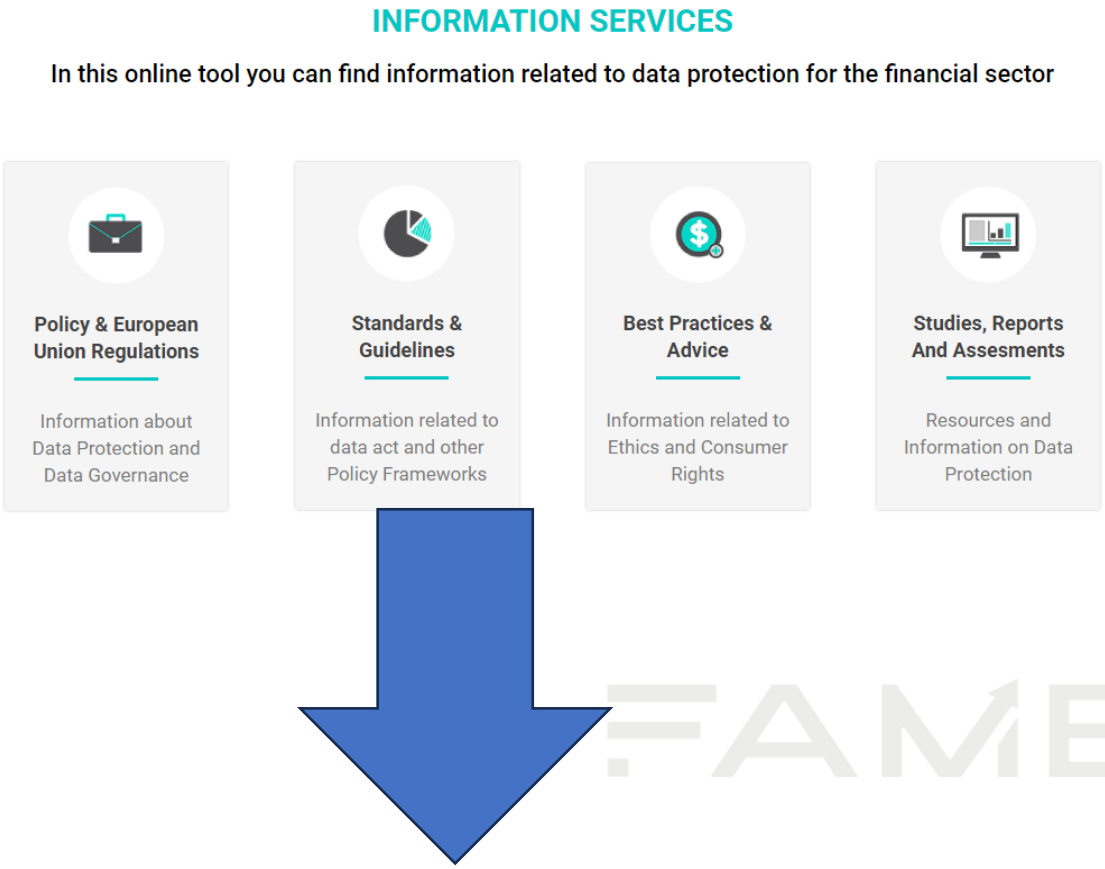
Using FAME website platform we envision a user-friendly website for communication the regulatory compliance tool framework to the stakeholders. The website includes an interactive tool for stakeholders to browse into regulatory framework and a download link for retrieving related laws and regulations. The main menu lists all related laws and regulations. FAME Regulatory Policy Framework Portal is a window to all related laws and regulation in the FAME ecosystem.

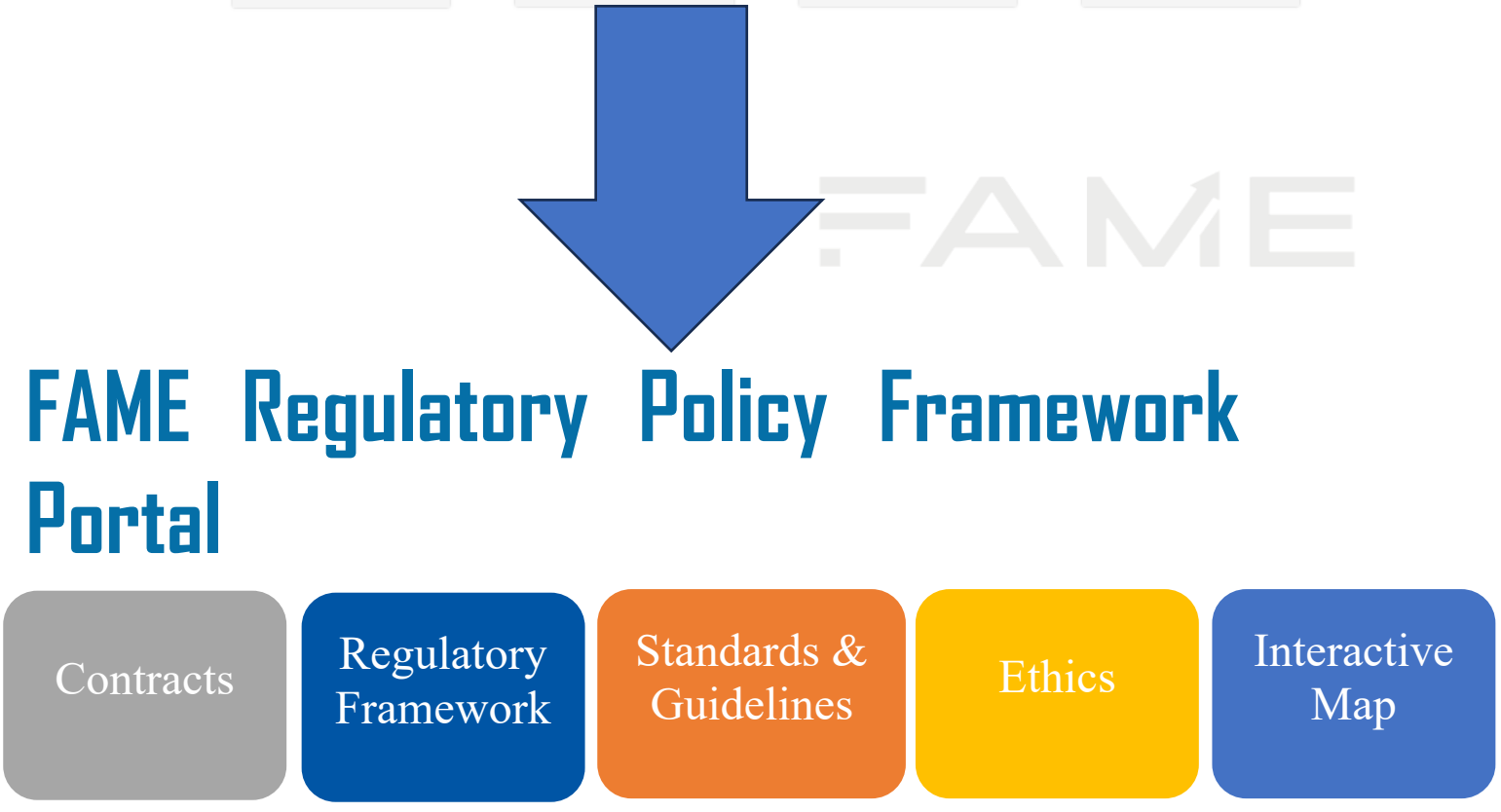
Link to FAME website

Download the regulatory compliance document.

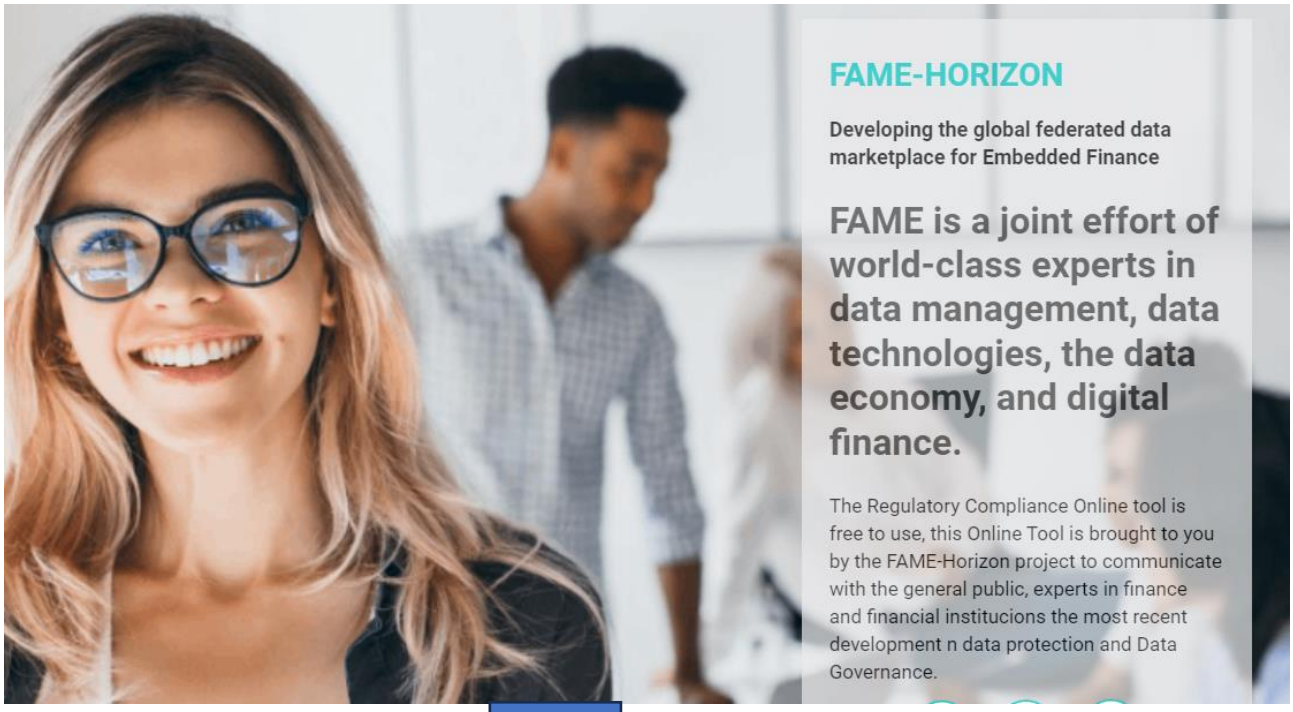
The main menu

This section of the tool provides information services. Users can extract information related to laws and regulation according to their need. This section categorizes information in an easy-to-use manner for the users. This section include information about laws and regulations, policies, standard and guidelines, best practices and advice, and studies, reports and assessments.



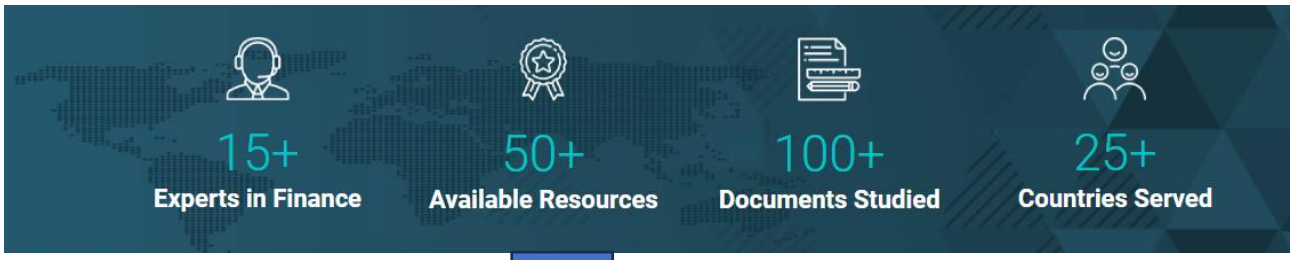


This section of the tool provides general and technical information about FAME. What is FAME, what is its goals and its achievements. There is a link to the main FAME project website for the users to explore more on the topic. The Regulatory Compliance Online tool is free to use, this Online Tool is brought to you by the FAME-Horizon project to communicate with the general public, experts in finance and financial institucions the most recent development n data protection and Data Governance.



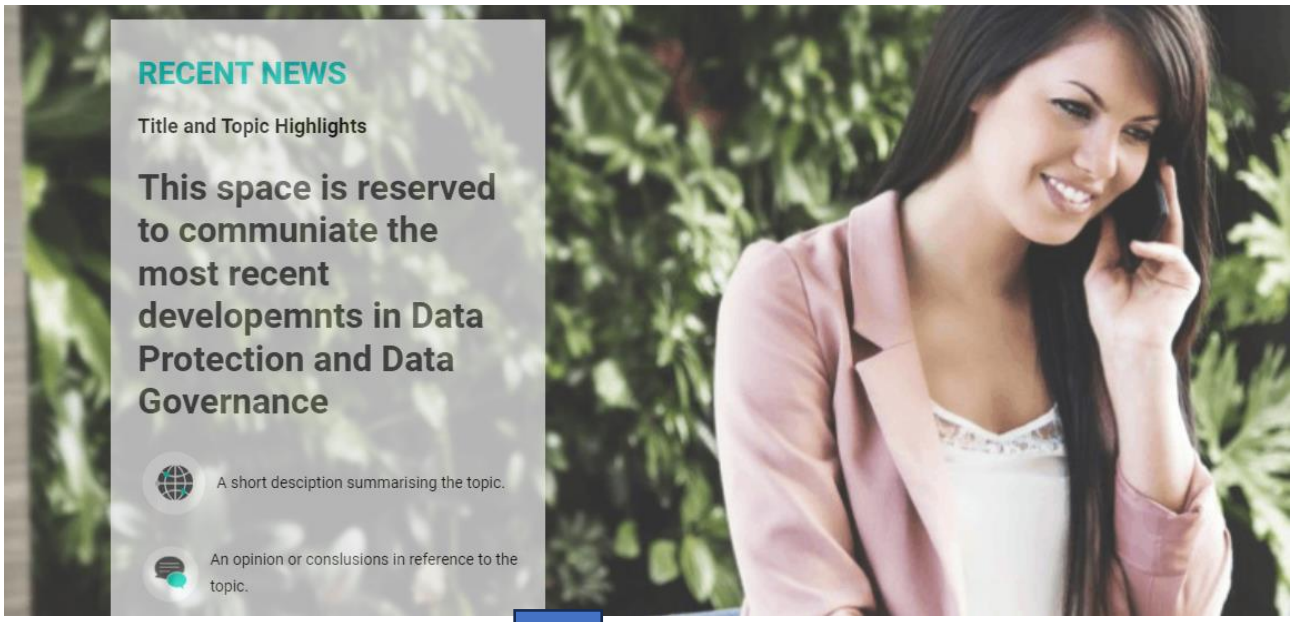
General and technical information about FAME

This section summarizes the main activities of the FAME project. It provides a snapshot of the number of experts in finance, number of available resources, number of documents studies, and numbers of countries served.



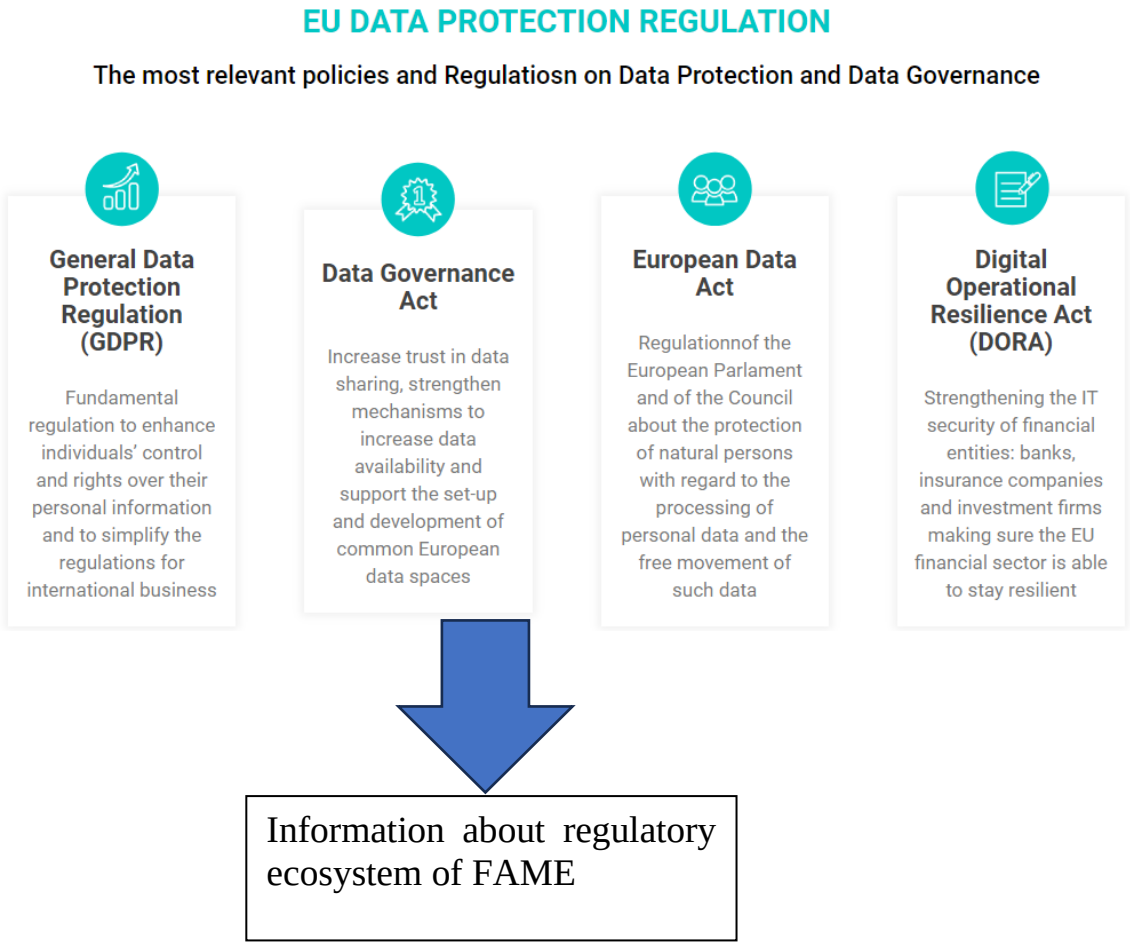
FAME project snapshot

This section provides information about recent news, and the FAME project public release. It is so vital to provide recent updates about regulatory ecosystem of the FAME project to keep the stakeholders engaged and up to date.



FAME project public release and recent news.

This section summarizes the EU data protection regulation. All related laws and regulations are listed in here with proper link to more details of each laws and regulations. The stakeholders can access the whole range of related information on each topic in a user-friendly way.



This section provides information about newly designed policy and regulations in an internation setting. Based on location of choice the related laws and regulations are listed with a detail information about related laws and regulations.

The FAME international background in a user-friendly setting.

5 Conclusions

In this deliverable we outline the mapping of the FAME project's regulatory compliance framework against similar European projects such as GAIA-X and IDSA. Then, we supply information about the related laws and regulations in the field. Finally, we present the prototype of the regulatory compliance tool website.

The regulatory environment of financial technology and embedded finance industry is ever changing. Therefore, it is vital to keep the stakeholder up to date in regards of related laws and regulations. The aim of this deliverable is to provide an overview of the related laws and regulation in full scope. We start by describing the positioning of the FAME project's regulatory framework in relation to similar European projects. Then, we deliver a full review of the seven most related laws and regulations in the field. We also describe a prototype of the regulatory compliance tool website.

Accessing the related laws and regulations in the field of finance in general and embedded finance in particular is easy. There is full access to the related laws and regulations on the European parliament website. However, defining the most relevant laws and regulations is cumbersome. We strive to provide a shprt description of each law and regulation in the regulatory environment follow up by a full description of the laws and regulation for the end users benefit.

6 References

[1] GDPR General Data Protection Regulation EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex (europa.eu)

[2] https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

[3] Data Act Data Act | Shaping Europe's digital future (europa.eu)

[4] DATA Act: OMB, Treasury, and Agencies Need to Improve Completeness and Accuracy of Spending Data and Disclose Limitations | U.S. GAO

[5] Data Governance Act / Open Data Directive The Data Governance Act & The Open Data Directive | data.europa.eu

[6] DORA Digital Operational Resilience Act (DORA) (europa.eu)

Publications Office (europa.eu)

[7] NIS2 The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament (europa.eu)

[8] PSD3/PSR + MIFID II + 4AMLD Introducing the PSD3, PSRs and FIDAR – reshaping the EU's regulatory framework on payment services and e-money - PwC Legal

[9] Consumer rights Consumer Rights Act 2022 (irishstatutebook.ie)