Commentary on the General Data Protection Regulation (GDPR)

by

Steptoe & Johnson LLP

for

BIPAR

The GDPR from an Insurance and Financial Mediation Perspective

July 2016
Contents

Foreword – BIPAR Chairman ......................................................................................................................................... 4
Foreword – Steptoe & Johnson ...................................................................................................................................... 5
I. Introduction .............................................................................................................................................................. 6
   What is the purpose of this commentary? .................................................................................................................... 6
   To whom is this commentary of interest? .................................................................................................................... 7
II. Legal Context .............................................................................................................................................................. 7
   Directive 95/46/EC (Data Protection Directive) ........................................................................................................... 8
   General Data Protection Regulation (GDPR) .................................................................................................................. 8
   Background .................................................................................................................................................................... 10
III. Protection of Personal Data under the GDPR ........................................................................................................... 13
   1. Definitions ............................................................................................................................................................... 13
      1.1. How does the legislation apply to intermediaries? .............................................................................................. 13
      1.2. What is “personal data?” ...................................................................................................................................... 16
      1.3. What is “data processing”? ................................................................................................................................... 16
   2. How to process data legally: balancing consent and legitimate interest .............................................................. 18
      2.1. Must intermediaries always obtain consent from individuals before processing personal data? ...................... 19
      2.2. What should intermediaries consider before relying on consent from individuals? ........................................ 19
      2.3. Can an intermediary rely on “performance of a contract” as a basis for processing personal data? .................... 20
      2.4. Can an intermediary rely on their “legal duties” as a basis for processing personal data? ................................. 21
      2.5. Can intermediaries rely on “legitimate interest” to process personal data? ....................................................... 21
      2.6. On what basis may an intermediary profile the data subject or a larger set of client data? ............................... 23
      2.7. Do intermediaries need to disclose both the legal basis and the purpose of processing? ................................. 24
      2.8. Can intermediaries further process data they have already collected? .............................................................. 24
      2.9. For how long should intermediaries retain personal data? ..................................................................................... 25
   3. What rights does the data subject enjoy? .................................................................................................................. 25
      3.1. The data subject’s right to access ........................................................................................................................ 26
3.2. The data subject’s right to be notified with certain data before processing takes place 28
3.3. The data subject’s right to rectification for inaccurate or incomplete information ....33
3.4. The data subject’s right to erasure (“right to be forgotten”) ......................... 34
3.5. The data subject’s right to restrict processing of data .................................. 34
3.6. The data subject’s right to take the data away (“portability”) ....................... 35
3.7. The data subject’s rights as regards profiling .............................................. 36
3.8. Restrictions on data controllers’ obligations and data subjects’ rights .......... 37
3.9. Access to redress .......................................................................................... 38

4.1. Do intermediaries need to appoint a Data Protection Officer? .......................... 39
4.2. Codes of conduct ....................................................................................... 41
4.3. Data controller record-keeping requirements ............................................. 43
4.4. Managing relations between joint data controllers .................................... 45
4.5. Managing relations between data controllers and processors .................. 45

5. Supervisory oversight ..................................................................................... 46
5.1. General ....................................................................................................... 46
5.2. Data breach ................................................................................................ 46

6. Consequences of intentional or negligent breach of the GDPR ......................... 48
6.1. Administrative fines ................................................................................... 48
6.2. Shared responsibilities ............................................................................... 49
6.3. Criminal law .............................................................................................. 49
6.4. Enforcement by other authorities ............................................................... 49
6.5. Supervisory cooperation ............................................................................ 50

7. Transfers of personal data outside the European Economic Area ................. 50
7.1. Has the Commission adopted an adequacy decision? ............................... 51
7.2. On what other legal basis may intermediaries send data overseas? .......... 51
7.3. How should intermediaries respond to third country court judgments or administrative authority decisions? .......................................................... 52
7.4. Next steps for international transfers ......................................................... 52

IV. Conclusion: A Checklist for Intermediaries .................................................. 54
Dear Reader,

The Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the so-called General Data Protection Regulation or GDPR) will impact all firms and persons who are dealing with “personal data”, including insurance and financial intermediaries.

The GDPR is a cross-sectoral text. It has not been drafted with the insurance or financial sector in mind, but it applies to the insurance and financial sector, including their intermediaries.

During the adoption process of the GDPR, BIPAR, in cooperation with its member associations, informed the EU legislators (European Parliament, Council of the EU) as well as the European Commission and the Supervisor, about requirements where the specificities of the insurance and financial sector needed to be taken into consideration to ensure that the stability and security of policyholders' insurance contracts will not be jeopardised. Some of our points were taken into consideration but the GDPR remains a complicated piece of regulation.

The intermediary sector is serious about the protection of its client data. In order to help intermediaries prepare for the new rules that will apply throughout the EU with effect from May 2018, BIPAR commissioned a Commentary on the GDPR from Steptoe & Johnson LLP, which clarifies data protection law in light of the changes brought about by the GDPR. Isabelle Audigier, BIPAR legal Director, and François Lestanguet, policy advisor, led BIPAR participation in this work.

Responsibility for compliance with all relevant EU and national legislation rests with individual firms and we hope that this Commentary will encourage market parties and also national regulators and data protection supervisory authorities to develop together a realistic framework and system of data protection in the EU.

André Lamotte
BIPAR Chairman

Nic De Maesschalck
BIPAR Director
Foreword — Steptoe & Johnson

The new EU General Data Protection Regulation is a complex, cross-sector text that will profoundly affect how insurance and financial intermediaries process personal data in the EEA (and beyond). It introduces numerous new concepts and requirements, whose interpretation – with input from competent authorities - will unfold over the next few years.

Steptoe & Johnson, LLP have been pleased to work with BIPAR in preparing a Commentary tailored to the needs of intermediaries and designed to help them comply with the new rules.

For over 30 years, lawyers in the Brussels office of Steptoe & Johnson, LLP have been advising professional associations, businesses and public bodies on a wide range of EU law questions. The Commentary’s authors are Guy Soussan and Philip Woolfson, EU Insurance Practice Group Partners, and Daniella Terruso, EU Policy Advisor and IAPP member.

This document and information provided herein do not constitute advice or recommendations regarding any individual situation and should not be relied upon as regulatory or legal advice or as a substitute for consultation with legal advisers or consultants.

For more information about Steptoe, visit www.steptoe.com
I. Introduction

What is the purpose of this commentary?

This document aims to help preparing for the application of the “Regulation of the European Parliament and of the Council 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)” – commonly referred to as the “General Data Protection Regulation” or “GDPR”. The GDPR has been published in the EU’s Official Journal, and will apply from 25 May 2018 throughout the European Economic Area (EEA). Like the Directive which it repeals, the GDPR is cross-sectoral and so has not been drafted with the insurance sector specifically in mind. This commentary has been prepared specifically to identify relevant provisions of the new legislation as they apply to Bipar members: i.e. intermediaries in the widest sense of the term: (re) insurance brokers, agents and Independent Financial Advisers (IFAs).

All intermediaries, whether large firms or small offices, use personal data to provide a variety of services to clients: to make quotations, arrange insurance cover and offer other financial products, manage claims, manage the client relationship, manage and conduct internal conflict checks. They also use this data for marketing and client profiling purposes, offering renewals, research and statistical analysis, crime prevention, credit assessment and other background checks, internal record-keeping, and meeting legal or regulatory requirements. Arranging insurance and other financial product coverage may require disclosures of personal data to insurers and other service providers such as consultants, market researchers, quality assurance companies, other companies in a corporate group, industry regulators, auditors and other professional advisors. This may require transfers of certain categories of personal data outside the EEA. Because of these activities, intermediaries are frequently “controllers” or “processors” of personal data and, thus fall within the scope of the legislation. Although data protection compliance is not new, the GDPR clarifies roles and responsibilities. Wherever

---

1 The EEA comprises the 28 Member States of the European Union, Iceland, Liechtenstein and Norway.
2 Description taken from Bipar’s GDPR Insurance intermediaries key messages of 25 June 2015.
3 This commentary uses these terms wherever appropriate.
possible this commentary highlights aspects where there is scope to alleviate the burden on small and medium sized enterprises.

To whom is this commentary of interest?

Generally, data protection legislation protects the personal data of identified or identifiable persons. When such a person resides in the EEA, they are referred to as a “data subject”. This commentary is primarily of interest to intermediaries established in the EEA. In numerous cases, such intermediaries already hold and are processing extensive personal data of data subjects, including transfers of personal data within the EEA and even beyond, in compliance with the Data Protection Directive (defined below). This commentary explains data protection law in light of the changes brought about by the GDPR. First, it summarises the legal context which has resulted in the adoption of the GDPR; it then describes and comments on key requirements of the GDPR as relevant to the insurance intermediary sector, as well as emphasises new duties for intermediaries; by way of conclusion and to help intermediaries prepare for the new rules, a checklist summarises the legislation and its application to intermediaries. This commentary is not legal advice and, therefore, for specific questions, intermediaries should take their own advice.

II. Legal Context

Protection of personal data has been a concern in Europe at least since the Second World War, both in the form of international treaties – the European Convention on Human Rights and the

---

4 On 24 June it was announced that the UK’s referendum on membership of the European Union resulted in victory for the leave campaign. At the time of editing, no notification triggering the withdrawal process had been made by the British Government. We expect the withdrawal process to take at least two years, and as the UK remains a full member of the EU until the process is complete, UK operators should continue to prepare to comply with the GDPR. After withdrawal, the GDPR will still apply to operators in the UK if they offer goods or services to EU citizens or if they monitor EU citizens’ behaviour. In addition, the UK will need to demonstrate that its legislation offers an adequate level of data protection, comparable to the GDPR, for data transfers between the UK and the EU.

5 i.e. the “Convention for the Protection of Human Rights and Fundamental Freedoms” opened for signature in Rome on 4 November 1950 and in force since 1953.
Council of Europe’s Convention 108⁶ — and under specific EU legislation referred to in the background section below. The GDPR is not, therefore, a revolution; rather, it has evolved from, and builds upon, existing texts. Nevertheless, the GDPR has new and important provisions, which this commentary explores.

- **Directive 95/46/EC** (Data Protection Directive)

Currently, this directive is the main legislative source for personal data protection in the EU. A directive is only binding as to the goal to be achieved and, furthermore, must be implemented into national law. In legislative practice, directives leave Member States flexibility to decide on how to achieve the goals. The Data Protection Directive is no exception and has led to differences in national implementing legislation. This Directive will no longer apply when GDPR comes into application.

- **General Data Protection Regulation (GDPR)**

*Directly applicable, binding nature*

The new rules are in the form of a regulation, which, by definition is, “binding in its entirety and directly applicable in all Member States”. Unlike directives, a regulation does not, therefore, need to be implemented into national law. Individuals and other persons can rely on it directly when enforcing their rights. The GDPR also repeals Directive 95/46/EC.

*Delegated acts*

The GDPR provides for acts, known as “delegated acts” and “implementing acts”. The Commission may adopt delegated acts in two areas, namely: standardised icons⁸; and

---

⁶ i.e. “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” signed in Strasbourg on 28 January 1981 and in force since 1985.

⁷ i.e. “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”.

⁸ A “standardised icon” is a symbol that represents an object or concept, e.g. a picture of an envelope used to represent an e-mail message. They are a method of providing information to data subjects of their rights as a picture.
certification requirements. The certification mechanisms will enable controllers and processors, including intermediaries, to demonstrate to external parties their “GDPR-compliance”.

The Commission may also adopt implementing acts on:

- standard contractual clauses to be inserted in “Data Processing Agreements” between data controllers and data processors and between data processors;
- codes of conduct, technical standards and mechanisms for certification;
- the adequacy of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation;
- standard data protection clauses;
- formats and procedures so that data controllers, data processors and supervisory authorities can exchange information electronically (for “binding corporate rules”);
- mutual assistance between supervisory authorities; and
- the formats and procedures for exchange of information electronically (for market monitoring, enforcement, etc.) among supervisory authorities and the European Data Protection Board.

**Member State flexibility**

Although the GDPR is a regulation, many of its provisions permit Member States to retain or introduce national rules. These provisions therefore risk diluting the uniformity of the GDPR’s rules. Any national law will, however, be interpreted against the principles set out in the GDPR and must also be notified to the Commission.

The Commission will regulate which information may be presented by such icons and the procedures for their approval. The term is specific to computing whereas for signs in public places, such as road signs, the term “pictogram” is more common.

---

9 Article 12(8), GDPR. Certification organisations must meet these requirements in order to offer certificates, seals and marks to data controllers and data processors; so that they, in turn, can demonstrate to the public that they comply with the GDPR.
10 Article 43(8), GDPR.
11 e.g. Article 23 on restrictions of rights and duties under the GDPR required to safeguard national security, defence, etc.
Supervisory cooperation

Although Member States enjoy flexibility to retain or introduce national rules, the current supervisory cooperation arrangements will change. The Article 29 Working Party\textsuperscript{12} will transition to a newly created European Data Protection Board (EDPB), whose tasks are defined in the Regulation\textsuperscript{13}, primarily to ensure consistent application of the Regulation across the EU by issuing guidelines, recommendations and best practices on a wide range of subjects. It will have legal personality and a secretariat, shared with the European Data Protection Supervisor (EDPS). National supervisory authorities will have to act collectively as a network. Together, they must ensure consistent application of the GDPR across the EU; for this purpose, may issue binding decisions, opinions, guidelines, recommendations and best practices, as well as provide advice to the Commission.

Background

This section summarises the main international treaties, concluded under the auspices of the Council of Europe. Though many members of the Council of Europe are also members of the EU, the Council of Europe is an international organisation which is separate from the EU. In relation to human rights and the protection of personal data, it traditionally has a significant influence on the EU, for example the European Convention on Human Rights forms part of EU law and is regularly cited in judgments on protection of personal data. Thereafter, this section focuses on the EU legal texts which underpin the GDPR.

- European Convention on Human Rights

This Convention guarantees the right to respect for private and family life, home and correspondence. Furthermore, it proclaims that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is

\textsuperscript{12} The Article 29 Data Protection Working Party comprises representatives of: each national supervisory authority/authorities; the European Data Protection Supervisor; and the Commission. The Working Party elects its chairman and vice-chairmen and a secretariat is provided by the Commission.

\textsuperscript{13} Article 70, GDPR.
necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.\(^{14}\)

- **Council of Europe Convention 108**

  This Convention is the first binding international instrument to protect the individual against abuses which may accompany the collection and processing of personal data and to regulate at the same time the cross-border personal data flow.

  In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of “sensitive” data on a person’s race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual’s right to know that information is stored on him or her and, if necessary, to have it corrected.

  Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

  The Convention also restricts cross-border flows of personal data to States where legal regulation does not provide equivalent protection.

- **Council of Europe recommendations**

  The Council of Europe periodically issues non-binding recommendations in relation to privacy and protection of personal data, for example Recommendation (2002)9E of 18 September 2002 on the protection of personal data collected and processed for insurance purposes.

- **EU Charter of Fundamental Rights**

  This charter establishes in EU law the fundamental rights set out in the European Convention of Human Rights referred to above. It became legally binding with the entry into force of the Treaty of Lisbon, in December 2009. In addition to the right to respect for his or her private and

\(^{14}\) Article 8, ECHR.
family life, home and communications\textsuperscript{15} first enshrined in the European Convention, the EU Charter also provides that everyone has the right to the protection of his or her personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to his or her data and the right to have it rectified. An independent authority must be able to control compliance of these rules\textsuperscript{16}.

\textsuperscript{15} Article 7.
\textsuperscript{16} Article 8.
1. Definitions

This section addresses practical questions: the extent to which intermediaries are within the scope of the new rules under the GDPR, and the definitions of personal data and data processing.

1.1. How does the legislation apply to intermediaries?

General definitions in the GDPR

As mentioned above, a “data subject” is an identified or identifiable natural (living) person\(^{17}\). “Personal data” is any information that relates to them.

A “data controller” is the natural or legal person, such as a company, that decides the nature and extent of a data processing operation\(^{18}\), i.e. the action\(^{19}\) involving a data subject’s personal data. A data controller is different from a “data processor”, who processes data on behalf of a data controller\(^{20}\), a role typically played by, for instance, an IT vendor or cloud computing service provider. In some EU Member States, intermediaries are confined to this role.

The GDPR permits “joint control”, for instance for an intermediary to jointly control the data processing operation(s) with an insurer, but the terms, particularly which entity is responsible for interaction with data subjects, must be set out in the contract and disclosed clearly to data subjects.

\(^{17}\) European Data Protection Authorities agree that only living beings are protected under the legislation. Article 29 Working Party (2007), Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p.22. Recital (14) GDPR states “Protection afforded by the Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.”

\(^{18}\) Article 4(7), GDPR.

\(^{19}\) See section 1.3.

\(^{20}\) Article 4(8), GDPR.
subjects. Although this is not new in Union law, not all Member States previously allowed intermediaries to be joint controllers, so in this sense, it is a new opportunity for intermediaries.

An EU "representative" must be appointed if an entity is located outside of the EEA but falls within the GDPR’s scope. An EU "representative" must be appointed if an entity is located outside of the EEA but falls within the GDPR’s scope.21 Two other parties are described in the GDPR, namely: a “recipient”, a person to whom personal data is disclosed; and a “third party”.

A recipient is typically a person working for an entity that is legally separate from the data controller or the data processor even if they are part of the same group or holding company, or it can be someone from a different division within the same entity.

A third party is a much narrower definition, i.e. “any person, other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data”. Only persons working for a legally separate entity will be considered a third party. In some Member States, intermediaries may be considered as third parties.

Why is the distinction between data controller and data processor important?

The GDPR applies to all data controllers and data processors established in the EEA as well as third-country entities that offer goods or services to, or monitor the behaviour of data subjects resident in the EEA. Responsibilities and liabilities differ, depending on the role the entity plays in the data processing.

Where an entity operates in more than one Member State, or also outside of the EEA, the distinction between whether it is a data controller or a data processor is also relevant to determine the entity’s main establishment and main supervisory authority. If an intermediary is a data controller, the location of its main establishment or decision-making will determine which jurisdiction is relevant for supervisory purposes; for a data processor, it will be the location of the main processing activity.

21 See Article 4(17). Article 3(2), GDPR sets out the territorial scope of the Regulation as including controllers and processors not established in the Union whose processing activities are related to either (i) offering of goods and services to data subjects in the Union (irrespective of payment) or (ii) monitoring the behaviour of such data subjects in so far as this behaviour takes place within the Union.
By way of example, in *Google Spain v. Costeja*\(^{22}\), the Court of Justice of the European Union upheld the right, for prosecution purposes, of a national supervisory authority to link an entity in the EU, however small and insignificant to the overall operations of the group, to a third country data controller or data processor established outside the EU.

### How do the definitions apply to intermediaries?

The definitions are functional, in that they depend on the role the intermediary plays in data processing. This means an intermediary will not always fall under one definition or another:

In some cases, an intermediary will be processing personal data on its own account. For instance, when the intermediary processes personal data about its employees, retains data about clients for its own records, or collects images of people, employees or the public, recorded by video surveillance (CCTV) cameras on its premises. The intermediary acts as a data controller.

In other cases, the intermediary as a data controller may engage a data processor to undertake certain aspects of processing, *e.g.* a corporate service provider for anti-money laundering reporting or payroll, advertising, data storage (including cloud computing), data security, or data destruction. The intermediary should therefore conclude a data processing agreement with the data processor (see section 4.5 for details).

To be considered a data processor, the intermediary will be subject to a data processing agreement concluded with a data controller. In practice, this means the intermediary should act only under clear processing instructions from a data controller. An intermediary may act as an insurer’s data processor, for example where the intermediary is appointed under a data processing agreement to act as administrator for the insurer and in accordance with the insurer’s instructions. The key requirements imposed on data processors are set out in section 4.5.

In yet other cases, an intermediary may be considered a recipient, *e.g.* if they are an employee of a data controller, but work in a separate division to the persons processing the data. An intermediary could be a third party to the data processing, if, for instance, they obtain the information in a context that is not connected to his or her employment\(^{23}\).

---

\(^{22}\) Court of Justice of the European Union, Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

\(^{23}\) The UK Information Commissioner’s Office (ICO) gives an example where an employee receives personal data to pursue a possible legal action not connected with their employment. In this case the employee is a third party in
1.2. What is “personal data”?

The GDPR only covers the processing of personal data, i.e. information that relates to a data subject. However, considering what could make a person identifiable, particularly when combined with other information, makes the scope potentially very broad. Examples include: name and address, social security number, health data and vehicle registration.

Certain special categories of data, often referred to as “sensitive data”, are subject to additional protections. The GDPR includes new health data, such as genetic and biometric data, within these categories.

Personal data related to offences and criminal convictions are treated separately in the GDPR. Intermediaries may process such data in order to prevent fraudulent claims, in particular when the processing is authorised by Union or Member State law.

Anonymous data is out of scope. The GDPR introduces a new regulatory regime for processing personal data that has undergone “pseudonymisation”. Although this data remains personal data, processing is subject to fewer obligations to encourage greater use of such techniques.

1.3. What is “data processing”?

**General definition**

“Processing” covers most activities involving personal data: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction. Therefore, any entity coming into contact with personal data is likely to be processing that data.

---

relation to their employer and the employer would have to have a specific legal basis for transferring the data to them.

24 Pseudonymisation is processing in such a way that the data can no longer be attributed to a specific data subject without the use of additional information which is kept separately and subject to safeguard measures.

25 Article 4(2), GDPR.
As applied to intermediaries

Intermediaries often process personal data for the following purposes:

- placing business with an insurer and managing the insurance contract (from the pre-contractual stage to termination of the policy or, even, post-termination);
- client management: business development, marketing and promotional activities;
- where criminal data is processed at the time the client is looking to sign up to a policy and is required to disclose any history of previous convictions, e.g. motor offences, or a burglary, or to assist in the management of litigation, e.g. to defend the intermediary and/or insurer or to defend the policyholder;
- detection or analysis of fraud, e.g. in the event of a forged client signature on an insurance policy document or analysis of an alert detected by tools placed on the intermediary’s network to prevent cyberattack; and
- in common with all economic operators, as an: employer; manager of premises, e.g. video surveillance; and network and security manager, e.g. surveillance tools to detect cyberattack.
2. How to process data legally: balancing consent and legitimate interest

This section sets out the legal basis and purposes for processing personal data where the intermediary acts as a data controller.

(Where the intermediary is a data processor, it should only process data in accordance with the agreement it has concluded with a data controller – see section 4.5).

Before processing personal data, an intermediary should check it has a legal justification for doing so i.e. (i) a valid legal basis and (ii) a specific purpose.

The legal bases - which are the same as the Data Protection Directive, but definitions have been refined - are:

- consent from the data subject;
- performance of a contract;
- fulfilment of a legal requirement;
- protection of the vital interests of the data subject or of another natural person;
- and
- 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. The balance of interest is weighted in favour of data subjects when they are children.\(^{26}\)

Special categories of personal data, such as genetic or biometric data may only be processed subject to specific safeguards according to Union and Member State law.\(^{27}\)

In practice, intermediaries are able to rely on: consent; performance of a contract; and legitimate interest as basis for processing of personal data.

\(^{26}\) Processing in order to perform a task carried out in the public interest or in the exercise of official authority vested in the controller is also a valid legal basis, but is not available to intermediaries.

\(^{27}\) See Article 9, GDPR. Recitals (10), (51), (52), (53), (71), (80), (91) and (97) are illustrative.
2.1. Must intermediaries always obtain consent from individuals before processing personal data?

Intermediaries will often, but not always, need to obtain consent before processing personal data.

The current rules – under the Data Protection Directive – already contemplate different forms of consent, depending on the category of data. The GDPR further defines consent.

In most cases, where consent is necessary, it should be a freely given, specific, informed and unambiguous\(^\text{28}\) indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify they agree to the processing of their personal data.

Where special categories of data are concerned, for instance for profiling\(^\text{29}\) or for certain transfers of personal data outside the EEA\(^\text{30}\), explicit consent\(^\text{31}\) is required.

2.2. What should intermediaries consider before relying on consent from individuals?

The difference under the GDPR from the Data Protection Directive is that consent is now a more difficult legal basis to rely on\(^\text{32}\). Consent is an important element of the legislation, providing data subjects with a measure of control over how their personal data is processed. Depending on the context, however, other legal bases may be more appropriate from both the controller’s and the data subject’s point of view. At its worst, consent may be illusory, a “take it

\(^{28}\) See Recital (32) which states that “clear affirmative action” is necessary, such as ticking a box on a website, statements or conduct that clearly indicate assent to all processing activities for a given purpose. Silence, pre-ticked boxes or inactivity do not constitute consent.

\(^{29}\) “Unambiguous” is specifically defined in the GDPR. It is the automated processing of personal data and is used to predict the following: performance at work; economic situation; health; personal preferences; interests; reliability; behaviour; location; or movements.

\(^{30}\) i.e. for transfer of personal data to a country without an adequacy decision and without any other legal basis.

\(^{31}\) The Article 29 Working Party has defined “explicit consent” as “all situations where individuals are presented with a proposal to agree or disagree to a particular use of disclosure of their personal information and they respond actively to the question, orally or in writing”.

\(^{32}\) As noted above in footnote 26, Recital (32) requires “clear affirmative action”. If the service is conditional on consent, the consent is not freely given and cannot be a legal basis for processing data. The data subject must be able to withdraw consent as easily as he or she has given it, meaning it is not a very stable basis for processing data as it could be withdrawn at any time by the data subject, leaving the intermediary with no legal basis to process the data.
or leave it” option, which erodes confidence and would, therefore, be an inappropriate basis for processing.

In an insurance context, the data subject needs to be made aware of the consequences of withdrawal of consent. These could be severe, for example termination of an insurance contract would lead to loss of protection and, possibly, exit charges. For health or motor insurance, it may not be possible to obtain new coverage with a new provider on similar terms, e.g. the loss of “no claims bonus” for motor insurance.

According to the context, performance of a contract, fulfilment of a legal requirement or legitimate interest may be more appropriate basis.

In cases where the data has not been derived directly from the individual, it may be more appropriate to notify the data subject, rather than obtain consent. The exact notification requirements are set out in section 3.2.

### 2.3. Can an intermediary rely on “performance of a contract” as a basis for processing personal data?

Both the Data Protection Directive and the GDPR recognise that this is a basis for processing personal data. It also covers processing in a pre-contractual relationship as long as it is “in order to take steps at the request of the data subject prior to entering into a contract”.

---

33 See Recital (40), GDPR.
2.4. Can an intermediary rely on their “legal duties” as a basis for processing personal data?

Private sector data controllers may be subject to a legal duty to process data, for example:

- In France, insurers are required to collect health data (injuries, medical certificates, and other supporting documentation, including the social security number) of the parties in a car accident. French law explicitly recognises that it may not be possible to obtain consent, as a basis for processing the data\(^ {34}\).

- In the UK, the Financial Conduct Authority requires insurers to maintain a register of employees and employee references numbers as a contingent action to support future asbestos claims. It is a legal requirement for intermediaries to collect this information.

- Throughout the EEA, employers must process social security and tax information about their employees.

Other legal duties may be less clear, for example whether this basis extends to foreign laws, such as a court order. Member States remain free to specify how this provision applies in their national law.

2.5. Can intermediaries rely on “legitimate interest” to process personal data?

Many controllers, including intermediaries, currently rely on this basis for processing personal data under the Data Protection Directive. “Legitimate interest of the controller” is also a basis for processing under the GDPR, but its scope is clarified. The intermediary must strike a balance between its interest as a controller and the rights of data subjects. The GDPR's recitals provide interpretation\(^ {35}\): the legitimate interests of a controller, including of a controller to which the data may be disclosed, or of a third party, may provide a legal basis for processing, provided

\(^{34}\) Article R.211-37 French Insurance Code as cited in the CNIL “Pack de conformité – Assurance” p. 11

\(^{35}\) See Recitals (47), (48) and (49), GDPR.
that the data subject’s interests, fundamental rights and freedoms do not override those of the controller. This requires consideration of: (i) the reasonable expectations of data subjects based on the relationship with the controller, as well as (ii) the time and context of the data collection.

Examples follow:

- Legitimate interest may exist based on a “relevant and appropriate relationship” e.g. the data subject is a client or in the service of the controller, including as part of a group of undertakings or institution affiliated to a central body;
- Processing to prevent cyberattack on the controller’s network, within the bounds of strict necessity and proportionality\(^\text{36}\) is a legitimate interest;
- Direct marketing or processing for the purposes of preventing fraud\(^\text{37}\).

In the event of dispute, the controller must demonstrate that their compelling legitimate interests override the interests, fundamental rights and freedoms of the data subject.

Case law from the Court of Justice of the European Union clarifies that national law may not add additional conditions to processing under this basis\(^\text{38}\). The GDPR confirms this strict approach thereby ensuring that the list of legal bases across the EU is exhaustive.

A data subject may object to processing (see sections 3.4 and 3.5), for example when a data controller sends e-mail communications to existing clients in order to promote its own or similar products or services. In such cases, the controller may send the e-mail, but must always provide the means for the data subject to “unsubscribe”. Repeatedly ignoring the wishes of the data subject could lead to complaint, which in the first instance is likely to be to the national data protection supervisor. It would be difficult for the controller to argue an overriding interest.

Whichever legal basis is chosen, the intermediary’s privacy notice\(^\text{39}\) must include and justify the choice of legal basis.

---

\(^{36}\) There are strict labour law requirements in many Member States, such as in France, regarding prior employee consultation before cyber security equipment may be deployed as well as limits to employers’ rights to look at the content of personal material, such as emails, even when saved on company equipment.

\(^{37}\) These examples are taken from the Recitals.

\(^{38}\) See Court of Justice of the EU, Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD, 24 November 2011 regarding a Spanish law rule which restricted processing under this basis only to information that was already in the public domain.
2.6. On what basis may an intermediary profile the data subject or a larger set of client data?

Profiling a data subject to assess their insurability is an integral part of setting policy terms. Section 3.7 discusses profiling in the context of data subjects' rights. Both the Data Protection Directive and the Council of Europe's Profiling and Direct Marketing Recommendations\(^{40}\) cover “automated decisions”, particularly those that have important consequences for data subjects. The GDPR defines profiling\(^{41}\) and provides data subjects with more extensive rights, i.e. to access their information, to be notified, to stop the profiling, and to avoid profiling-based decisions which produce legal or similar effects.

If an intermediary intends to take decisions based (solely) on automated processes which either produce legal effects or similarly significant effects, e.g. a fully automated on-line insurance policy quotation, it should choose one of following legal bases:

- Necessary for the performance of the contract;
- Authorised by Union or Member State legislation to which the controller is subject and which contains suitable safeguards\(^{42}\); or
- Based on explicit consent of the data subject.

The data subject must be able to contest the decision. Additionally, the data processed must not contain any special category data, such as health data, unless:

- the data subject has explicitly consented to processing for one or more specified purposes (unless the purpose is banned under Union or Member State legislation); or
- processing is necessary in the substantial public interest under Union or Member State legislation, is proportionate to the aim pursued, respects the essence of the right to

---

\(^{39}\) A privacy notice informs data subjects about use of personal data by entities and about the rights of data subjects under applicable legislation. It also enables entities to fulfill their legal obligation to provide fair processing information to data subjects. The notice is typically distributed on the public-facing website of the entity.

\(^{40}\) Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010);
Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985).

\(^{41}\) See Article 4(7), GDPR.

\(^{42}\) Suitable safeguards include rights to request that a human review the decision, rights for the data subject to express a point of view and to contest the decision.
data protection and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

2.7. Do intermediaries need to disclose both the legal basis and the purpose of processing?

The intermediary should always disclose the purpose of the processing to the data subject. It is possible to have – and disclose - multiple purposes e.g. processing to arrange insurance cover and combat fraud. Disclosure enables data subjects to exercise their rights, principally to access their data. As under the Data Protection Directive, the GDPR prohibits secret or covert processing of data, unless specifically permitted in law.

2.8. Can intermediaries further process data they have already collected?

A data controller may be contemplating further processing of the data for a purpose other than the one for which the data have been collected, for example having collected the data for fraud prevention, the intermediary may wish to use the data for a secondary purpose e.g. new policy quotation. The test of whether the new purpose is compatible with the initial one depends on: (i) whether there is an identifiable link between the two purposes; (ii) whether, given the circumstances, a data subject could reasonably expect a data controller to re-process the data in this way; (iii) the consequences of the re-processing for the data subject; and (iv) the safeguards the data controller envisages to mitigate potential harm or detriment to the data subject. If the further processing is incompatible with the initial purpose, the data controller must ensure the legal basis continues to be sound, and disclose any change to the legal basis that is necessary to the data subject. The controller must also disclose the new purpose to the data subject.

43 The “Insurance Link” investigation by the Irish Office of the Data Protection Commissioner in 2011 resulted in the recommendation, inter alia, that personal data concerning insurance claims collected for the purposes of fraud prevention and pooled by insurers should not be further processed for policy quotation purposes. The Commissioner said that further processing would only be possible if the insurers were to put in place appropriate provisions and safeguards.
2.9. For how long should intermediaries retain personal data?

The GDPR restricts the time that personal data may be retained, i.e. "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".

An intermediary lawfully can retain relevant and necessary data for longer periods where data has been anonymized or pseudonymised⁴⁴ (requirements to safeguard pseudonymised data apply).

3. What rights does the data subject enjoy?

Data subjects have enforceable rights against entities processing their data. Currently, under the Data Protection Directive, such rights place responsibilities and liabilities on data controllers. Under the GDPR, an intermediary which is a data controller must facilitate exercise of the data subject’s rights⁴⁵, including by giving directions to a data processor through a data processing agreement.

As explained at section 6 below, the GDPR extends liability for wrong-doing and harm to data processors. This means that the data subject can sue data processors jointly with, or separately from, the data controller.

---

⁴⁴ This is a technique whereby personal information data fields within a database are replaced with artificial identifiers, or pseudonyms, e.g. names are replaced by a unique number. In theory, only the database owner has the key to re-identify the data subjects. Care should be taken that others cannot re-identify the data subjects using publicly available information. An infamous case 1997 concerned on-line “anonymous” medical records in Massachusetts where researchers could re-identify data subjects, including the governor, William Weld, using publicly available voter registration data as the key.

⁴⁵ See Article 12(3), GDPR.
3.1. The data subject’s right to access

If the intermediary is a data controller, data subjects have the right under the Data Protection Directive and the GDPR to request personal data that relates to them that the controller is processing. The GDPR sets EU-wide controller requirements and should, therefore, make duties much clearer for cross-border operators.

3.1.1 What information should the data controller provide?

Data subjects should be informed in advance that their personal data will be processed. The most common form of notification is a privacy notice. Under the GDPR, the information must include:

- where the data will be processed;
- how to access the data;
- the purpose of the processing;
- the categories of data processed;
- the recipients or categories of recipient to whom the data have been or will be disclosed, particularly if the data will be transferred outside the EU (in this case, the data subject must also be informed of the safeguards taken to protect the data pursuant to the transfer);
- for how long the data will be stored, or if it is not possible to state this, the criteria that will be used to determine the period, e.g. the length of time the insurance policy is in force;
- information on how to exercise the right to lodge a complaint to a national supervisory authority;
- if the data have not been collected directly from the data subject, an indication as to the source;
- whether automated decision-making, including profiling, is part of the processing as well as further information about it, i.e. “meaningful information about the logic
involved”, the significance and likely consequences of such processing for the data subject.

A copy, either in paper or electronic form, must be provided for free\(^\text{46}\).

Data controllers should provide the requested information without undue delay (within one month\(^\text{47}\)) or provide reasons why it does not intend to comply with the request. This harmonises the timescale to react to access requests across the EU for the first time. For additional copies of the data, a “reasonable fee based on administrative costs” may be charged. There is no time limit for data subjects to exercise this right\(^\text{48}\).

The right to access is subject to the following:

- The “overriding legal interests” of others may prevent a data controller from divulging the personal data, or may mean only partial disclosure of the personal data is appropriate because the rights and freedoms of others must not be adversely affected by the disclosure. This is no different from the Directive, so existing national guidance is likely to continue to apply;

- A data controller may not generally refuse to act on a request. In order to refuse, he or she must demonstrate the request was “manifestly unfounded” or “excessive”. The GDPR comments that “repetitive” requests may fall within this definition. Cases have arisen calling into question the purpose of subject access, and which could provide grounds for a refusal to provide information \(^\text{49}\). The Data Protection Directive’s provisions allow a summary to be provided; the GDPR refers to a “copy” and this will need to be interpreted. In any event, the data controller should inform the data subject why the request has been refused in whole or in part;

\(^{46}\) This is a more onerous duty than under the Data Protection Directive, which only requires data controllers to provide a summary of the data in an appropriate format, and allows them to charge a small administrative fee.

\(^{47}\) Recital (59), GDPR. The term “month” is not defined. It is not clear whether it means calendar month, 31 days, or business days, etc. Complex cases or multiple requests may be dealt with within three months.

\(^{48}\) See, for instance, Court of Justice of the EU, C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 7 May 2009.

\(^{49}\) See, for instance, Court of Justice of the EU, Joined Cases C-141/12 and C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M. and S. The main purpose of these cases was to access the minutes regarding the applicants’ request for a residence permit. The Court held that a summary in an intelligible format was sufficient to comply with the Data Protection Directive and safeguard the data subjects’ rights under the Charter of Fundamental Rights. The applicants did not gain rights to the administrative document (the minutes) using these legal bases.
• Where the data controller has reasonable doubts about the identity of the requester, they should request additional information to confirm the identity before responding to the request; and

• The general public interest50: any restriction based on this ground must be necessary in a democratic society and proportionate to the aim pursued. Member States are required to strike a balance between the rights of data subjects and the freedom of controllers to run a business.

The Commission is empowered to develop guidance under a delegated act to assist data controllers in providing information to data subjects, in particular as regards the use of standardised icons51.

3.2. The data subject’s right to be notified with certain data before processing takes place

All data subjects, whether the data controller has a direct relationship with them or not, have the right to receive similar information (see sections 3.2.1 and 3.2.4 respectively). Typically, this is provided in a privacy notice.

The main difference between direct and indirect relationships is the timing of when the pre-processing notification should be made (sections 3.2.2 and 3.2.5). Limited waivers exist (sections 3.2.3 and 3.2.6-7).

3.2.1 What information should controllers provide to clients and other data subjects with whom they have a direct relationship?

• the data controller’s identity and contact details, including, where possible, the controller’s representative in that Member State and/or contact details of the data protection officer;

• the purposes of the processing and the legal basis;

50 Article 23, GDPR.
51 See footnote 7.
where the processing is based on “legitimate interests” pursued by the controller or by a third party, the controller should set out those interests;

where applicable, the recipients or categories of recipients of the personal data; and

where applicable, whether the controller/processor intends to transfer personal data to a third country or international organisation and, if so, (i) whether the Commission has adopted a decision as to the adequacy of the protection of personal data by that third country or organisation, or (ii) any other basis for the transfer and the means to obtain a copy of the documentation or where this has been made available.

In addition, the data controller should inform the data subject about the following:

- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period, e.g. the duration of the insurance contract;

- the data subject’s rights, i.e. to request: (i) access and rectification or (ii) erasure or restriction of processing or (iii) to object to the processing as well as (iv) the right to data portability (where applicable – see section 3.6);

- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- how to exercise the right to complain to a national supervisory authority;

- whether the data subject must provide the personal data as part of a statutory or contractual requirement, or a requirement necessary to enter into a contract;

- whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and

- whether the data will be subject to automated decision-making including profiling and “meaningful information about the logic involved”, as well as the significance and the consequences of such processing for the data subject.

### 3.2.2. When should this information be given to the data subject?

At the time the personal data are obtained.

---

52 Article 13(2)(f), GDPR.
Where the controller intends to further process the personal data for a new purpose, the controller should ascertain whether the new purpose is compatible with the initial one. If not, before going ahead, the controller should provide the data subject with information on the new purpose and any relevant further information (e.g. if a new legal basis is required).

3.2.3  *What waivers may apply?*

Where the data subject already has the information.

3.2.4.  *What information should data controllers provide to data subjects with whom they have no direct relationship?*

Sometimes intermediaries do not have a direct relationship with the data subject whose data they need to process in their or the insured’s interest, for example where the data subject is: (i) the passenger, pedestrian or driver, other than the insured, in a car accident; (ii) the beneficiary of a life insurance policy; (iii) household members, other than the insured home owner, for home insurance; and (iv) family members whose medical conditions may have to be disclosed during an assessment for a family health or combined travel insurance policy.

The notification requirements under the GDPR are essentially the same as for those with whom a data controller has a direct relationship (see above) but the notification timing will differ (see below - 3.2.5).

3.2.5.  *When should data controllers give the notification information to the indirect data subject?*

The controller must provide this information either:

- within a reasonable period after obtaining the data, but at the latest within one month, having regard to the specific circumstances in which the data are processed;
- if the data are to be used to communicate with the data subject, at the latest at the time of the first communication to that data subject; or
- if the data are to be disclosed to another recipient, the data subject should be informed at the latest when the data are first disclosed.

As above, where the controller intends to further process the data for a new purpose, before going ahead, the controller should provide the data subject with information on the new purpose and any relevant further information.
3.2.6  Do any waivers apply?

- where the data subject already has the information; or
- where provision proves “impossible” or would involve “a disproportionate effort”; in such cases the data controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available; or
- obtaining the information or disclosure is expressly laid down by Union or Member State law to which the controller is subject\(^5\), which provides appropriate measures to protect the data subject’s legitimate interests; or
- where the data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Additionally, Recital (26), GDPR refers to certain objective factors that can be deployed in the intermediary's favour, i.e. “…the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments....”

Finally, there is no need to maintain, acquire or process information to identify a data subject if the sole purpose is to comply with the GDPR itself\(^5\).

3.2.7  How can I rely on “impossibility” or “disproportionate effort” to not notify the data subject?

These terms are not defined in law, but already appear in the Data Protection Directive.

Although the Court of Justice of the European Union has interpreted these terms no case fully clarifies whether an intermediary could decline to notify a data subject with whom they have no direct relationship.

\(^5\) e.g. UK intermediaries' obligation to collect personal health data about work-related asbestos.

\(^5\) Article 11, GDPR. See also Recital (57), GDPR "If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.”
Impossibility

The Court considered what may constitute impossibility in the Sumitomo appeal case\textsuperscript{55}. The appellant claimed impossibility \textit{i.e.} that the President of the Court of First Instance had effectively required the appellant to adduce evidence demonstrating “with absolute and complete certainty that it would suffer serious and irreparable damage”. This is a stringent test (which was rejected by the Court on the facts of the case).

Disproportionate effort

This term has been interpreted in relation to the right of a data subject to access to data and disclosure to third parties, rather than notification to data subjects. Nevertheless, some of the criteria may prove useful in determining what might constitute disproportionate effort. In the case of Rotterdam v. Rijkeboer\textsuperscript{56}, the Court referred to relevant provisions of the Data Protection Directive, \textit{i.e.} Recital (40) which mentions the number of data subjects and the age of the data and Article 17 on security of processing, which states that Member States should require that the controller implements appropriate technical and organisational measures, having regard to the state of the art and the cost of their implementation. GDPR Recital (62) also refers to the number of data subjects and the age of the data as well as any appropriate safeguards adopted. As regards security of processing, Article 32 states that, in addition to state of the art and implementation costs, 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 are all relevant considerations.

In sum, pending specific commentary by the authorities, “impossibility” and “disproportionate effort” require a case-by-case analysis, using criteria such as those suggested above, and duly recorded in the intermediary’s records.

\textsuperscript{55} Court of Justice of the European Union, Case C-236/07, Sumitomo Chemical Agro Europe SAS v. Commission, 23 January 2008.

\textsuperscript{56} Court of Justice of the European Union, C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, 7 May 2009.
3.3. The data subject’s right to rectification for inaccurate or incomplete information

Where data is incorrect or incomplete, the GDPR gives the data subject the right to have the data corrected. The data controller should act without undue delay to comply, including by issuing a supplementary statement confirming to the data subject that it has rectified or completed the data.

57 Previously, data subjects had to rely on national law.
3.4. The data subject’s right to erasure (“right to be forgotten”)

A request to have data erased from a data controller’s records is usually based on a claim that the processing is unlawful, or is being processed for a new purpose, which has not been pre-disclosed to the data subject. The burden of proof is on the controller to refute this.

Under the GDPR a data subject may require erasure if:

- the data are no longer necessary for the purpose(s) for which they have been processed;
- consent has been withdrawn and there is no other legal basis to process the data;
- the data subject objects to the processing and it is not possible to argue overriding legitimate grounds of the data controller or other party;
- the data processing has no legal basis; or
- the data should be erased to comply with a legal obligation in Union or Member State law to which the data controller is subject.

Restrictions to these rights apply, where the processing is necessary, in particular:

- for compliance with a legal obligation under Union or Member State law to which the data controller is subject; or
- for the establishment, exercise or defence of legal claims.

3.5. The data subject’s right to restrict processing of data

The GDPR imposes new requirements on data controllers, as follows:

- Where the accuracy of the data is in question, the data controller should only store it, and not process it in any other way, until it has been able to verify accuracy;
- Where the processing is unlawful, the data subject must be able to choose between erasure or restriction;
- Data controllers must retain data for the establishment, exercise or defence of legal claims when these data are needed by the data subject (even if the data are no longer needed by the data controller);
- Where the legitimate grounds for processing by the data controller are in question, processing should be restricted to storage, pending verification by the controller. In
these cases, any processing other than storage may only be carried out under the following conditions:

- with the data subject’s unambiguous consent;
- for the establishment, exercise or defence of legal claims;
- for the protection of rights of another natural or legal person; or
- for reasons of important public interest of the Union or a Member State.

Like for processing a data subject’s access request, the data controller may not charge a fee for this service.\(^\text{58}\)

### 3.6. The data subject’s right to take the data away (“portability”)\

This is a duty only on data controllers: only for specific data, (personal data provided to the controller by the data subject); and only in set circumstances (where data processing is based either (i) on the data subject’s consent or (ii) on performance of a contract; and (iii) the processing is carried out by automated means). For such data, data subjects may request a copy “in a structured, commonly used, machine-readable and interoperable format”, so that they can give that data to another data controller. The intention is to enable data subjects to shop around the digital economy for different commercial service providers. This differs from the access rights discussed above, which apply to all data. Restrictions apply:

- where the processing is based on another legal basis;
- data portability should not prejudice the rights of other data subjects; and
- Union or Member State law may impose restrictions, as far as they are necessary and proportionate in a democratic society.

Further guidance will be necessary from both national authorities and, possibly, the EDPB.

---

\(^\text{58}\) See Recital (59), GDPR.
3.7. The data subject’s rights as regards profiling

In a data protection context, profiling means: (i) the automated processing of personal data; and (ii) using those data to evaluate certain personal aspects relating to that data subject, e.g. “aspects concerning the person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location and movements”.

The GDPR recitals state that, in particular profiling underlies an intention to take decisions about the data subject or to analyse or predict personal preferences, behaviours and attitudes. It is related to, but distinct from, direct marketing.

The GDPR requires data controllers to:

- inform data subjects of the consequences of profiling decisions (see above regarding notification requirements);
- conduct impact assessments where data are processed with the intention of taking decisions about specific data subjects and after any systematic and extensive evaluation of their personal data (i.e. profiling decisions); and
- enable data subjects to exercise their full rights of access, notice, objection, cessation and avoidance in relation to profiling decisions.

Where profiling is used to take a decision “which produces legal effects or similarly significantly affects” a data subject, intermediaries must exercise particular care, for example:

- An underwriting decision for an insurance policy may rely on external data such as an individual’s credit rating and this, in turn, may raise the questions: (i) whether such data constitute profiling; (ii) if so, whether the data subject can claim the right to challenge the decision or whether the profiling decision is unavoidable. In all likelihood Member State law will apply, and the EDPB will issue guidance.

Such decision-making will only be allowed when:

- it is necessary for performance of a contract between the data subject and the data controller;
- it is expressly authorised by Union or Member State law, subject to safeguards (such as human intervention to “correct” any machine error);
• it is based on the data subject’s explicit consent (provided the data subject has the right to object or to revoke consent at any time).

Should an intermediary wish to continue to process data despite a data subject’s objections, as data controller they will have to demonstrate “compelling legitimate grounds which override the data subject’s rights”. Marketing is not an overriding legal basis.

Profiling is further restricted for special categories of data, *e.g.* health data (decisions based on profiling must be necessary and meet specified criteria). Profiling children’s data is banned.

### 3.8. Restrictions on data controllers’ obligations and data subjects’ rights

Under the GDPR, Member States may adopt exemptions and restrictions in relation to data protection rights and duties. Certain restrictions are relevant to intermediaries. Member States may, for example, restrict data protection provisions in order to safeguard interests such as:

- important objectives of general public interest of the Union or of a Member State, an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; or

- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions\(^59\).

This means that data subjects may not be able to exercise their rights and that data controllers, such as intermediaries, may be exempt from their duties to notify or disclose that they are processing personal data. Subject to local rules, an example of an exception would be a breach of rules on international sanctions or other restrictive measures. Where Member States propose national legislation to restrict data subject rights, they must ensure the legislation is necessary and proportionate to pursue a legitimate aim. As a general matter, any national law based on “general public interest” is still subject to review – including by the Court of Justice of the European Union – under EU law and general fundamental rights.

\(^59\) Article 23, GDPR.
3.9. Access to redress

The GDPR grants data subjects rights to take action against data controllers and data processors as well as the decisions of the European Data Protection Board (EDPB) and national Data Protection Authorities (DPAs). They can complain to a DPA, but also have the right to judicial remedy. Data subjects can appoint a legally recognised not-for-profit body, organisation or association\(^{60}\) to act on their behalf.

Data subjects also have a right to compensation for material or non-material damage as a result of a breach of the Regulation. The notion of “material or non-material” damage will be interpreted broadly in line with case-law of the Court of Justice of the European Union.

---

\(^{60}\) These entities must have “statutory objectives which are in the public interest” and they must be “active in data protection”.
4. Privacy programme management: What does an intermediary need to do?

The GDPR emphasises actively managing privacy. This is termed “accountability” in the GDPR and comprises three major requirements: (i) a defined role for data protection officers; (ii) more extensive record-keeping within entities, including notification of data breaches; and (iii) dynamic contract management, in particular between controllers and processors.

Professional associations and other bodies representing controllers and processors are encouraged by Article 40 to assist their members with meeting their obligations under GDPR by introducing codes of conduct or encouraging members to sign up to voluntary accredited certification schemes (see section 4.2).

4.1. Do intermediaries need to appoint a Data Protection Officer?

The GDPR requires certain data controllers and data processors to appoint a data protection officer (DPO), defined as “a person with expert knowledge of data protection law and practices and the ability to fulfil the tasks” if any of the criteria, as set out below, are met. The DPO assists the data controller or data processor to monitor internal compliance with the GDPR. The DPO does not have to be an employee, and “should be in a position to carry out his or her duties in an independent manner.” A group of undertakings may share a single DPO, provided the individual is “easily accessible from each establishment”.

Appointment is mandatory if the data controller or data processor is:

- A public authority or body; or
- Where the core activities of the data controller or data processor involves “regular and systematic monitoring” of data subjects on a “large scale”;

---

61 The criteria are set out in Article 39.
62 There is no definition of “large scale”. EDPB may examine this point to ensure consistent application of the Regulation across the EU. See EDPB tasks, in particular Article (70)(1)(e).
• Where the core activities of the data controller or data processor involves processing on a “large scale” categories of data relating to either the special categories (sensitive data) or criminal convictions and offences.

Intermediaries may fall into the second or third scenario but it remains unclear as to whether all intermediaries would fall into either category.

Other than the categories set out above, associations may, either on their own initiative, or as required by Union or Member State law, designate a DPO to act for the association. In practice, given the requirements to have expert knowledge of law and practice as applicable to the establishments in question, this represents a significant commitment. By way of example, a multi-entity, multi-jurisdictional DPO will need several languages and detailed knowledge of several legal disciplines, e.g. employment, data subject law, etc. The DPO must enjoy sufficient authority within an entity, in addition to the specific responsibilities inherent in the role.

Criteria for DPO appointment could be one of the first opinions given or aspects examined by the EDPB for consistent application across the EU. Some national supervisors are expected to press for appointment of mandatory DPOs, subject to objective criteria such as the type of data processed, volume of data or nature of activity of the processing entity.

Small and medium-sized enterprises (SMEs) may merit special consideration since the GDPR expressly refers to their specific needs.

---

63 See Article 37(5) for DPO qualification requirements. The GDPR is silent on whether existing certifications such as the IAPP’s CIPP/E or CIPM will suffice or whether a certain number of years of experience will be required, e.g. 15 years.

64 See Article 38, GDPR: proper and timely involvement in all relevant issues; sufficient resources to carry out tasks; role as contact point for data subjects; independence and protection against sanction by employer, professional secrecy and confidentiality.

65 See Article 39, GDPR: counselling regarding applicability of the legislation; monitoring compliance, awareness raising and training of staff; carrying out audits and impact assessments; and liaison with national supervisory authorities.

66 Article 64(2), GDPR provides that any supervisory authority, the Chair of the EDPB or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the EDPB with a view to obtaining an opinion.

67 Article 70(1)(e), GDPR provides that the EDPB may examine, on its own initiative, on request of its members or on request of the Commission, any question covering the application of the Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of the Regulation.

68 Recital (13).
4.2. Codes of conduct

As mentioned above, professional associations and other bodies representing controllers and processors may prepare codes of conduct, or amend or extend existing codes to specify how the GDPR applies to their sector. One of the many EDPB tasks is to encourage the drawing up of codes of conduct\textsuperscript{69}.

Recital (81) encourages the use of codes by stating that “adherence of the processor to an approved code of conduct ... may be used as an element to demonstrate compliance with the obligations of the controller”. Recital (148) on penalties, including administrative fines, notes that in imposing a fine, “due regard should however be given, [inter alia] to ... adherence to a code of conduct and any other aggravating or mitigating factor”.

Such codes may cover:

- fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to the public and to data subjects:
  - the exercise of rights of data subjects;
  - the information provided to, and the protection of, children and the manner in which the consent of parents and guardians may be obtained;
- measures and procedures in relation to controller responsibilities, data protection by design/default and security measures;
- data breach notification procedures to supervisory authorities and to data subjects;
- international data transfers; or
- out-of-court proceedings and other dispute resolution mechanisms\textsuperscript{70}.

\textsuperscript{69} Article 70(1)(n).
\textsuperscript{70} Article 40(2)(a)-(k), GDPR.
Such codes should be open to both controllers and processors in a given sector (referred to, in the GDPR, as “categories”) and contain binding and enforceable commitments. They may be open to non-EU members so to provide appropriate safeguards for international data transfers\(^\text{71}\). Compliance monitoring should be built in\(^\text{72}\). They may be either restricted to national boundaries, in which case, the national DPA must examine and approve, register and publish it before it has any status under the GDPR\(^\text{73}\). If the code relates to processing activities in several Member States, the EDPB must examine and approve it and submit its opinion to the European Commission. The Commission may decide, by way of an implementing act, that the code has general validity in the Union\(^\text{74}\), i.e. that relevant actors in a given sector from any of the 28 Member States may sign up to the code.

Once approved, the professional association or representative body should be accredited by the national DPA to monitor compliance of the code by participating members\(^\text{75}\). It would be responsible for taking action in cases of infringement by a participating member, including suspending or striking that member from the list of code members\(^\text{76}\). This would be without prejudice to the national DPA’s own tasks and powers, including its independent role in taking action against organisations that infringe the GDPR.

\(^{71}\) Article 40(3), GDPR.
\(^{72}\) Articles 40(4) and 41, GDPR.
\(^{73}\) Article 40(5) and (6), GDPR.
\(^{74}\) Article 40(7)-(10), GDPR.
\(^{75}\) Article 41 (1), GDPR.
\(^{76}\) Article 41(4), GDPR.
4.3. Data controller record-keeping requirements

4.3.1. Risk assessment and impact assessment

Before a controller processes data, it should decide, with its DPO, how risky the processing is likely to be to the rights and legitimate expectations of data subjects. If the risk is high, the controller should carry out an impact assessment to evaluate the origin, nature, particularity and severity of the risk. Examples include: processing using new technology; innovative techniques, such as profiling; and large-scale processing of special categories of data or data relating to criminal convictions and offences.

Where the high risk cannot be mitigated by the data controller by appropriate measures (technology or implementation), it should consult its national supervisory authority before going ahead with the processing. The authority will respond within a defined period. Supervisors will draw up and publish lists of processing which are and are not likely to require an impact assessment. The EDPB may then consolidate these lists. It would be in intermediaries’ interest to input to this process.

4.3.2. Policy making

Data controllers must have in place “appropriate data protection policies, technical and organisational measures” to prevent unlawful processing, and undertake audits to demonstrate compliance, including documentation showing that the controller has considered “the effectiveness of the measures”.

4.3.3. Security

Data controllers must take measures that are commensurate with the state of the art and costs of implementation, taking into account the nature, scope, context and purposes of the processing, as well as the risk to data subjects.

Appropriate technical and organisational measures may include:
• pseudonymisation and encryption of personal data;
• measures to ensure the confidentiality, integrity, availability and resilience of systems and services;
• measures to restore availability and access following a physical or technical incident; and
• processes to regularly test, assess and evaluate the effectiveness of the measures in place.

The GDPR encourages entities to sign up to approved codes of conduct and/or certification schemes to demonstrate compliance. The ISO 27000 family of standards, for instance, is likely to be an accredited scheme that would help intermediaries demonstrate that they keep information assets secure.

Further guidance is likely from either national DPAs or the EDPB. Meantime, the EDPS has issued guidance in its advisory capacity to the EU institutions and bodies. Although the guidance is not based on the GDPR, but on Regulation 45/2001 which is specifically for the EU institutions and bodies, it is inspired by “generally accepted good practice in Information Security Risk Management”, and is, therefore, of potential use to all data controllers.

4.3.4. **Data processors**

The GDPR imposes certain obligations directly on data processors, rather than through the data processing agreement imposed by the data controller, for example data processors are also bound to keep records of data processing.

---

4.4. Managing relations between joint data controllers

As noted in the definitions section 1, the GDPR allows two or more controllers to jointly agree the purposes and means of processing. To avoid confusion, the controllers must define their respective roles and relationships, such as which party will notify data subjects (e.g. of the identity and contact details of the controllers) so that data subjects may exercise their rights. This definition must be set out “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. The essence of the arrangement must be made available to data subjects.

4.5. Managing relations between data controllers and processors

As noted in the definitions section 1, the GDPR distinguishes between data controllers and processors. They should set out their relationship in a data processing agreement. Data controllers may only use data processors that provide sufficient guarantees that they will implement appropriate technical and organisational measures to keep personal data secure.

The GDPR specifies the key contractual requirements of the data processing agreement. As noted in section II, the Commission may adopt an implementing act on standard contractual clauses to be included in the data processing agreement.

Additionally, data processors must not sub-contract without “prior specific or general written consent of the data controller”.

Finally, the administrative fines, set out in section 6.1., apply to data processors as well as data controllers.

79 Articles 13 and 14 information to be provided to data subjects when the data is collected from the data subject and where the data is collected from a third party.
80 Article 26, GDPR.
81 Article 28(3) requires a contract or other legal act under Union or Member State law, that is binding on the processor with the regard to the controller and stipulates the strict terms and conditions of the processing.
5. Supervisory oversight

5.1. General

As noted in section 1.1, relations between supervisors and controllers change significantly under the GDPR. On the assumption that a more “mature” relationship should develop between supervisors, controllers and processors, the GDPR has dispensed with the previous requirement to notify processing to the supervisor. The GDPR does, however, now require entities to manage their internal privacy programmes actively as set out at section 4.

5.2. Data breach

A breach is defined as “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”\(^{82}\).

*Data controllers*

Data controllers must inform their national supervisory authority within 72 hours from discovery of an incident.

They must notify:

- the nature, categories and approximate number of data subjects, categories and number of data records;
- the name and contact details of the DPO or other contact point;
- the likely consequences of the breach; and
- the measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.

\(^{82}\) Article 4(12), GDPR.
**Data processors**

Data processors should inform their data controller of a breach as soon as they become aware of it, *i.e.* without undue delay.

This requirement is likely to be part of the data processing agreement. It could result in disputes between the data controller and processor, particularly if there are claims arising as a result of the breach.

5.2.1. *Should all breaches be notified?*

The GDPR states that only data breaches that could result in a “risk to the rights and freedoms of data subjects” need to be notified. However, this definition is very broad and it is not clear when there would not be a risk. Guidance will be necessary from either national authorities or the EDPB.

5.2.2. *What should the data controller notify to data subjects in case of a high-risk breach?*

In high risk situations[^3], and in close cooperation with the supervisory authority, the data controller should also inform affected data subjects about a data breach “without undue delay or as soon as reasonably feasible”.

Data controllers must notify the nature of the breach and at least:

- the name and contact details of the DPO or other contact point;
- the likely consequences of the breach; and
- the measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.

The Article 29 Working Party has produced guidance on personal data breach notification in relation to the e-Privacy Directive[^4].

5.2.3. *What should data processors notify to the data controller?*

The controller has a duty to use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet GDPR requirements, including for the security of processing. In case

[^3]: This is currently undefined.
of data breach, the GDPR imposes a direct duty on data processors to report, but it does not set out details of the reporting, which are therefore governed by the data processing agreement (see section 4.5).

The GDPR provides that the data processing agreement must stipulate that the processor assist the controller in ensuring compliance with breach notification requirements taking into account the nature of the processing and the information available to the processor. Membership of an approved code of conduct may be an element to demonstrate that the processor has provided sufficient guarantees to implement appropriate technical and organisation measures and that the processing meets the requirements of the GDPR to protect data subjects’ rights. Breach notification procedures are a potential element to include in any future binding and enforceable code of conduct for the insurance intermediary sector, whether a national or cross-border code.

6. Consequences of intentional or negligent breach of the GDPR

6.1. Administrative fines

Drawing on experience in sanctions under competition rules, the GDPR sets uniform administrative fines; they are significant and DPAs can impose them on both data controllers and data processors. Where the legal system of a Member State does not provide for administrative fines, it should ensure that fines imposed are effective, proportionate and dissuasive.

Fines for intentional or negligent breach of the GDPR range between €10,000,000 and 2% of annual worldwide turnover and €20,000,000 or 4% of such turnover.

DPA decisions to impose fines depend on the circumstances of each individual case – consideration is likely to be made for natural persons and small and medium sized enterprises (SMEs). The GDPR states that for a minor infringement, or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a DPA may issue a reprimand. Where the fines are imposed on non-commercial undertakings, the DPA should take account of

---

85 Article 28, GDPR.
the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of fine.

6.2. Shared responsibilities

A controller or processor may be liable to persons who have suffered damage as a result of unlawful processing or of any act which is incompatible with the GDPR. In particular joint and several liability means responsibility is shared between the data controller and the data processor, unless either party can prove they were not responsible for the act giving rise to the damage. Where both are found liable, either party could be held responsible in court for the entire damage. This is to ensure data subjects have access to effective compensation. The party held jointly and severally liable must then claim the sum corresponding to the other party’s share in separate legal proceedings. Data processors need to be particularly careful not to act outside of the authority granted to them under the data processing agreement.

6.3. Criminal law

Recital 149 confirms that Member States have full flexibility to continue to impose or to introduce criminal sanctions in particular for infringements which are not subject to administrative fines as set out in the GDPR, or for breaches of national implementing legislation. Any sanctions should not breach the principle of *ne bis in idem* (double jeopardy).

6.4. Enforcement by other authorities

A breach of the GDPR does not preclude other enforcement action against a data controller or processor; likewise, enforcement action by other authorities – for example, an authority that regulates intermediaries – does not preclude enforcement action by a DPA. Breach of the GDPR by an intermediary could, therefore, result in sanctions under the GDPR and under other regulatory texts, for example regulating the intermediary’s conduct of business, systems and controls or administrative procedures.
6.5. Supervisory cooperation

The European Data Protection Board (EDPB) is the main EU decision-making body, with legal personality, at the centre of GDPR governance. It comprises a Chair, one head of the supervisory authority in each Member State and the European Data Protection Supervisor (EDPS). The Commission will participate in its activities without voting rights. A secretariat will be shared with the EDPS. Its main task will be to contribute to consistent application of the GDPR, including by advising the Commission particularly in the preparation of decisions on the adequacy of protection in third countries and promoting cooperation between supervisory authorities. To this end, it will issue guidelines, recommendations and best practices.

The EDPB will play a leading role in approval of pan-European codes of conduct as it will be required to adopt an opinion on any draft code and submit this to the Commission. It will also participate in establishing certification schemes, privacy seals and marks to assist entities to demonstrate compliance with the GDPR.

As noted in section II, the Commission may complete the legal framework underpinning supervisory cooperation by adopting implementing acts on:

- mutual assistance between supervisory authorities; and
- the formats and procedures for exchange of information electronically (for market monitoring, enforcement, etc.) among supervisory authorities and the EDPB.

7. Transfers of personal data outside the European Economic Area

Data controllers and processors may only transfer personal data to third countries or international organisations if data subjects will enjoy an adequate level of protection for their personal data. Transfers depend on the methods set out below.

---

86 See footnote 76.
87 This 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 such as the United Nations, the OECD, the FSB, IOSCO, IAIS, etc.
7.1. Has the Commission adopted an adequacy decision?

The Commission may decide that an entire territory or sector(s) in a third country offers an adequate level of protection. Where the Commission has adopted an adequacy decision under the Data Protection Directive, transfers of personal data may continue under GDPR to those jurisdictions without any further need for authorisation.88

An adequacy decision is not, however, free from challenge. In October 2015, in the Schrems case89, the Court of Justice of the European Union annulled the Commission’s decision regarding the adequacy of the Safe Harbour arrangements between the EU and US. At this stage, it is not clear whether the EU-US Privacy Shield, which replaces Safe Harbour, will be adopted and remain free from challenge.

7.2. On what other legal basis may intermediaries send data overseas?

In the absence of an adequacy decision, a data controller or data processor (acting under the data controller’s authority), may still transfer data to a “non-adequate” jurisdiction by relying on alternative safeguards. These comprise:

- Binding corporate rules: these cover a corporate group or group of enterprises engaged in joint economic activity and must be approved in advance by a supervisory authority; or
- Standard contractual clauses that have either been adopted or authorised by the Commission or a national supervisory authority.

Like the Data Protection Directive, the GDPR offers additional legal bases (derogations), as follows:

88 Article 45(9) states that decisions adopted by the Commission on the basis of the current Directive shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with the GDPR. Few decisions have been taken so far: Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, United States - EU-US Safe Harbor (annulled, Privacy Shield pending adoption), and Eastern Republic of Uruguay.

89 Court of Justice of the European Union, Case C-362/14, Maximilian Schrems v Data Protection Commissioner, 6 October 2015
Data subject explicit consent;
Performance of a contract;
Legal claims;
Vital interest (such as to save a life or physical integrity);
Legitimate interest (restricted to non-repetitive and residual cases where no other legal basis applies90); and
Public interest, such as international tax information exchange, exchange between financial supervisory authorities, etc.

7.3. How should intermediaries respond to third country court judgments or administrative authority decisions?

Transfers of personal data in response to a third country court judgment or decision of an administrative authority must be based on a mutual legal assistance treaty. Intermediaries may need to strike the right balance between EU and Member State national data protection law and other jurisdictions’ compliance obligations (e.g. anti-money laundering/anti-bribery legislation).

7.4. Next steps for international transfers

As noted in section 7.1, the Commission intends to adopt a replacement adequacy decision for transfers to the USA. The Schremss case has, in turn, cast doubt over aspects of the alternative safeguards for transferring data where no adequacy decision has been taken, namely binding corporate rules and standard contractual clauses (see section 7.2). The doubt is due to revelations that clauses in these safeguards may have been used to compel private companies to provide personal data for government surveillance purposes. The safeguards may have to be amended to reflect this case-law.

90 Both the supervisory authority and the affected data subjects must be informed.
91 See footnote 89.
As noted in section II, the Commission may also complete the framework under GDPR by adopting implementing acts on:

- the adequacy of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation;
- standard data protection clauses; and
- formats and procedures so that data controllers, data processors and supervisory authorities can exchange information electronically (for “binding corporate rules”).
IV. Conclusion: A Checklist for Intermediaries

In view of the complexity of the new rules set out in the GDPR and by way of conclusion to this commentary, this section sets out a checklist of points for the insurance intermediary sector, as follows:

What is the General Data Protection Regulation/GDPR?

- The GDPR replaces the Data Protection Directive –It is binding in its entirety and directly applicable in all Member States of the European Economic Area (EEA)
  - 9 Chapters
  - 90+ Articles
  - 250+ pages
  - Much greater detail than in previous EU legislation
  - It will apply from 25 May 2018 throughout the EEA

What are the key definitions that intermediaries need to be aware of?

- Intermediaries are often either a “data controller”: a natural or legal person that decides the nature and extent of data processing; or a “data processor”: a person that processes data on a data controller’s behalf. The definitions depend on the role the intermediary plays in data processing. They are important because responsibilities and liabilities differ, depending on the designation.

- The GDPR permits “joint control” which is not new in Union law but not a role that all Member States previously allowed, for instance, allowing intermediaries to share control with an insurer. This is a new opportunity for intermediaries.

- The definition of “personal data” is unchanged from the Directive, i.e. information that relates to a living, identified or identifiable natural person – a “data subject”.

THE GDPR FROM AN INSURANCE AND FINANCIAL INTERMEDIATION PERSPECTIVE
• The special categories of personal data are amended, *e.g.*
  
  o **health data** covers all data pertaining to the consumer’s health status
  
  o restrictions are placed on processing data related to **offences and criminal convictions**.

• “Data processing” covers most activities involving personal data. Any intermediary coming into contact with personal data, for instance placing business with an insurer and managing the insurance contract, is likely to be processing that data and would be subject to the GDPR.

**On what basis can an intermediary legally process personal data?**

• The legal bases are largely the same as the Directive, but definitions have been refined.

• Data subjects must be notified of the legal basis (and the purpose of the processing).

• The following legal bases are commonly used by intermediaries:
  
  o consent from the data subject;
  
  o performance of a contract;
  
  o fulfilment of a legal requirement;
  
  o legitimate interest pursued by the controller or by a third party.

• Special categories of data, such as health data, may only be processed with explicit consent from the data subject.

• Further processing: a data subject, such as an insured, may agree to their personal data being processed for the purposes of applying for a policy, but this does not necessarily constitute consent for additional processing purposes *e.g.* marketing new products. Intermediaries should consider, in advance, whether the new processing is compatible with the initial legal basis.

• Personal data should only be retained for specified periods.
How should an intermediary safeguard data subjects’ rights?

- Intermediaries should provide clear information to data subjects to facilitate the exercise of rights:
  - within deadlines set out in the GDPR:
    - controllers must act without undue delay, at least within 1 month of receipt of a request (+ two further months for complex/multiple cases)
    - action = either information provision or giving the reasons why the request is rejected.
  - information must be provided free of charge unless manifestly unfounded or excessive (repetitive). In this case, a reasonable fee may be charged.
  - information may be provided in combination with standardized icons to give a meaningful overview of the intended processing
- Intermediaries need to notify data subjects of the legal basis and purpose of the processing (both direct/indirect data collection)
- Intermediaries should facilitate access to data that relates to data subjects (without prejudice to the rights of others), rectify inaccurate and incomplete data, and erase data on request (“the right to be forgotten”). A controller that has made the data public must take reasonable steps to inform each recipient to whom the data were disclosed that the data subject has requested erasure, unless it would be impossible or involve disproportionate effort.
- Intermediaries should refrain from processing personal data e.g.
  - where the data subject contests the accuracy, or
  - where the data subject has objected to the processing (i.e. unless the legitimate grounds of the controller override the data subject’s rights).
  - A data subject cannot prevent an intermediary from processing data for the purposes of a legal obligation, such as anti-money laundering background checks or fraud, or from retaining data for the purposes of the defence of a legal claim against the intermediary. However, it may be possible for the data subject to request that processing of this data be restricted, pending review.
Intermediaries that are controllers should give effect to data subjects’ right to “data portability” if the data is processed on the basis of, for instance, performance of a contract. This may mean intermediaries should provide information to insureds so that they can give it to a new service provider.

Intermediaries should be aware that data subjects may object to processing, including profiling, unless the controller can demonstrate:

- compelling legitimate grounds, or
- that the processing is necessary for legal claims

Data subjects may seek administrative and judicial redress against intermediaries in connection with these safeguards to data subjects’ rights.

**Spotlight on data subjects’ rights with regard to profiling**

What is new?

- profiling definition;
- intermediaries should notify data subjects about profiling;
- intermediaries should obtain explicit consent from the data subject (to process personal and special categories of data).

As previously, individuals have the right to object where intermediaries use electronic means to arrive at a decision which:

- produces legal effects concerning them, or
- similarly, significantly affects them.

These provisions do not apply where processing is:

- necessary for performance of a contract;
- authorised by Union or Member State law (with safeguards); or
- based on the data subject’s explicit consent.
Privacy programme management - What are the differences between the Directive and the GDPR?

- Intermediaries may have to appoint a Data Protection Officer;
- Professional associations representing intermediaries may prepare codes of conduct containing binding and enforceable commitments to specify how the GDPR applies to their sector;
- Intermediaries that are controllers should conduct a risk assessment before processing data, and for high risk processing, conduct an impact assessment and consult the national Data Protection Authority;
- Intermediaries that are controllers should have appropriate policies and technical/organisational measures in place to prevent unlawful processing. Audits to demonstrate effectiveness and compliance are necessary;
- Intermediaries, whether they are controllers or processors should have appropriate security measures in place to protect personal data;
- Relations between joint data controllers and between controllers and processors must be clearly defined from the outset;
- New data breach notification requirements for both intermediaries, whether controllers or processors are set out in the GDPR;
- Transfers of data outside the EEA are still strictly regulated. Intermediaries should ensure they undertake international data transfers using one of the following: Adequacy Decisions, Binding Corporate Rules and Model Clauses. The EU and US are currently negotiating a new mode of transfer, the "Privacy Shield", which may be available shortly.
Intentional or negligent infringement of the GDPR – What should intermediaries be aware of?

- Intermediaries should be aware that the GDPR harmonises sanctions for unlawful data processing or other infringements of the legislation. This includes:
  - Administrative fines;
    - Fines for intentional or negligent breach of the GDPR range between €10,000,000 and 2% of annual worldwide turnover and €20,000,000 or 4% of such turnover, depending on the infringement.
- Intermediaries may also be subject to criminal law, depending on the Member State of operation;
- Any wrong-doing may also draw unwanted attention from other agencies for failure to have proper systems and controls in place;
- GDPR encourages coordinated action by supervisory authorities;
- Intermediaries should review their own insurance coverage to ensure they have adequate cybersecurity provision.

July 2016

Copyright © 2016 Bipar. No part of this document may be reproduced without permission.