EN

Article 4.

Definitions

Article 4.

For the purposes of this Regulation:

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

Recitals

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as 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. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion Nº 4/2007 on the concept of personal data (2007).

Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (2008).

> Data outlining the use of the service can be divided into different categories:
>
> - the query logs (content of the search queries, the date and time, source (IP address and cookie), the preferences of the user, and data relating to the user's computer);
> - data on the content offered (links and advertisements as a result of each query);
> - and data on the subsequent user navigation (clicks).
>
> Search engines may also process operational data relating to user data, data on registered users and data from other services and sources such as e-mail, desktop search, and advertising on third party websites.

An individual's *search history* is personal data if the individual to which it relates, is identifiable

Though *IP addresses* in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.

When a cookie contains *a unique user ID*, this ID is clearly personal data.

ANNEX 1 contains example of data processed by search engines.

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (2014).

Data Protection Commission (Ireland), Guidance Note: Anonymisation and Pseudonymisation (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020):

9. There are two principal sources of location data available for modelling the spread of the virus and the overall effectiveness of confinement measures:
– location data collected by electronic communication service providers(such as mobile telecommunication operators) in the course of the provision of their service; and
– location data collected by information society service providers' applications whose functionality requires the use of such data (e.g., navigation, transportation services,etc.).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020):

18. The term "*user*" is typically used to refer to individuals who are registered with the service, i.e. those who have an "account" or "profile". Many social media services can, however, also be accessed by individuals without having registered (i.e. without creating an account or profile). Such individuals are typically not able to make use of all of the same features or services offered to individuals who have registered with the social media provider. Both users and non-registered individuals may be considered "*data subjects*" within the meaning of Article 4(1) GDPR insofar as the individual is directly or indirectly identified or identifiable.

Case Law

CJEU, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs*, C-70/10 (2011).

CJEU, *Worten – Equipamentos para o Lar SA/Autoridade para as condições de trabalho*, C-342-12 (2013).

CJEU, *YS/Minister voor Immigratie, Integratie en Asiel*, C-141/12 and C-372/12 (2014).

CJEU, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources*, C-293/12 and C-594/12 (2014).

CJEU, *Breyer/Germany*, C-582/14 (2016).

CJEU, *Nowak/Data Protection Commissioner*, C-434/16 (2017).

CJEU, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Manni*, C-398/15 (2019).

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

Guidelines & Case Law

Documents

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> The behavioural advertising methods often entail the processing of personal data. This is due to various reasons:
>
> i) behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. **In other words, such devices enable data subjects to be 'singled out', even if their real names are not known.**
>
> ii) Furthermore, the information collected in the context of behavioural advertising relates to, (i.e. is about) a person's characteristics or behaviour and it **is used to influence that particular person**. This view is further confirmed if one takes into account the possibility for profiles to be linked at any moment with directly identifiable information provided by the data subject, such as registration related information.

DPC (Ireland), Guidance for Organisations Accidentally in Receipt of Personal Data (2020):

> An organisation, whether in the public, private or voluntary sector, must be aware of the possibility of finding itself accidentally in possession of personal data. The broad definition of '**processing**' in Article 4(2) of the GDPR means that opening, transmitting, deleting or simply storing personal data that you have unintentionally acquired will bring the GDPR into play.

DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).

Case Law

CJEC, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07 (2008).

CJEC, *Lindqvist*, C-101/01 (2003).

CJEU, *Schwarz/Stadt Bochum*, C-291/12 (2013).

CJEU, *La Quadrature du Net et al./Premier ministre et al.*, C-511/18, C-512/18, C-520/18 (2020).

CJEU, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs*, C-623/17 (2020).

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

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

Guidelines & Case Law

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018):

> Profiling is composed of three elements:
>
> - it has to be an automated form of processing;
> - it has to be carried out on personal data; and
> - the objective of the profiling must be to evaluate personal aspects about a natural person.
>
> Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.
>
> Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.
>
> The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.
>
> A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.
>
> The GDPR is inspired by but is not identical to the definition of profiling in the Council of Europe Recommendation CM/Rec (2010)132 (the Recommendation), as the Recommendation excludes processing that does not include inference. Nevertheless

the Recommendation usefully explains that profiling may involve three distinct stages:

- data collection;
- automated analysis to identify correlations;
- applying the correlation to an individual to identify characteristics of present or future behaviour.

Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:

- ability to perform a task;
- interests; or
- likely behaviour.

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

Recitals

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as 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. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for

attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

Guidelines & Case Law

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

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

Guidelines & Case Law

Case Law

CJEU, *Tietosuojavaltuutettu/Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17 (2018).

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

Guidelines & Case Law

Document

Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (2008).

> A *search engine provider* that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the *controller*, since he effectively determines the purposes and means of the processing.

Article 29 Working Party, Opinion 2/2010 on behavioural advertising (2010):

> When behavioural advertising entails the processing of personal data, ad network providers also play the role of **data controller**. Ad network providers have complete control over the purposes and means of the processing.

> However, the publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their websites. This is because the publishers facilitate such transfer and co-determine the purposes for which it is carried out, i.e. to serve visitors with tailored adverting. In sum, for these reasons, publishers will have some responsibility as **data controllers** for these actions.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (2010).

ICO, Guidelines Data controllers and data processors (2014) – Guidelines by the British Supervisory Authority ICO.

CNIL, Guide for processors (2017) – Guidelines by the French Supervisory Authority CNIL.

European Data Protection Supervisor, *Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (2019).

EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).

EDPB, *Guidelines 7/2020 on the Concepts of Controller and Processor in the GDPR* (2021).

EDPB, Guidelines 8/2020 on the targeting of social media users (2020).

Data Protection Commission (Ireland), Data Protection Considerations Relating to Receivership (2020):

> The 'controller' of personal data is the entity that determines the 'purposes and means' of processing personal data – i.e. '**why**' and '**how**' the personal data is processed.

Case Law

CJEU, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16 (2018).

CJEU, *Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV*, C-40/17 (2019).

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

Guidelines & Case Law

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" *(2010).*

CNIL, Guide for processors (2017) – Guidelines from the French Supervisory Authority CNIL.

European Data Protection Supervisor, *Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (2019).

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Recitals

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

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

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

Recitals

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only

to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Guidelines & Case Law

Document

EDPB, *Guidelines 5/2020 on Consent under Regulation 2016/679* (2020).

Case law

CJEU, *Schwarz/Stadt Bochum*, C-291/12 (2013).

CJEU, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV/Planet49 GmbH*, C-673/17 (2019).

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

Guidelines & Case Law

Article 29 Working Party, Guidelines on Personal Data Breach Notification Under Regulation 2016/679 (2018):

> In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles:
> – "Confidentiality breach" – where there is an unauthorised or accidental disclosure of, or access to, personal data.
> – "Integrity breach" – where there is an unauthorised or accidental alteration of personal data.
> – "Availability breach" – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

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

Recitals

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person

which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Guidelines & Case Law

Article 29 Working Party, Working Document on Genetic Data (2004).

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

Guidelines & Case Law

To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is "resulting from specific technical processing relating to the physical, physiological or behavioural characteristics".The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.

In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person".
To sum up, in light of Article 4.14 and 9, three criteria must be considered:

— **Nature of data**: data relating to physical, physiological or behavioural characteristics of a natural person,

— **Means and way of processing**: data "resulting from a specific technical processing",

— **Purpose of processing**: data must be used for the purpose to uniquely identifying a natural person.

EDPB, Guidelines 3/2019 on processing of personal data through video devices — 2019

Article 29 Working Party, Opinion 03/2012 on developments in biometric technologies (2012).

Article 29 Working Party, *Opinion 02/2012 on facial recognition in online and mobile services* (2012).

Article 29 Working Party, Working document on biometrics (2003).

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

Recitals

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2011:088:TOC

Guidelines & Case Law

Documents

EDPB, Guidelines 3/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak, (2020).

(16) 'main establishment' means:

Recitals

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main

establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

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

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

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

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

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

Recitals

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

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

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

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

Recitals

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

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

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

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

(23) 'cross-border processing' means either:

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

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

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

Guidelines & Case Law

Documents

EDPB, Guidelines on relevant and reasoned objection under Regulation 2016/679 (2020).

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [19];

[19] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2015:241:TOC

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

General Data Protection Regulation (EU GDPR)
The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679). Source: EUR-lex.

Related information Article 4. Definitions

Recitals

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as 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. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk,

medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

[9] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45). https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=OJ:L:2011:088:TOC

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.