20 March 2018

Factsheet on the key issues relating to the relationship between the proposed ePrivacy Regulation (ePR) and the General Data Protection Regulation (GDPR)

1. Purpose & Introduction

As the ePrivacy Regulation aims to complement and particularise the GDPR, this factsheet outlines the GDPR provisions that are most likely to be relevant for the negotiations. It also contains an Annex with all the provisions referenced in this document.

The GDPR will be applicable from 25 May 2018, replacing the existing Data Protection Directive (95/46/EC). In 99 Articles and 173 Recitals, it imposes detailed obligations on those that are processing personal data.

2. Definitions

The GDPR applies to the **processing** of **personal data**.

Personal data means any information relating to an **identified or identifiable** natural person (referred to as the 'data subject')—this is a person who **can be** identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data or an **online identifier** (Art. 4(1)). The GDPR states that such online identifiers may include IP addresses, *cookie identifiers* or other identifiers such as radio frequency identification tags, as all of these may leave traces which, particularly when combined with other information received by the servers, may be used to create profiles of the individuals and identify them (Recital 30).

To work out whether a data subject is 'identifiable', account should be taken of '*all the means reasonably likely to be used...either by the controller or by another person to identify the natural person directly or indirectly*', such as singling out.

The GDPR does not apply to anonymous information, or to personal data which has been anonymised in such a way that the data subject is not or no longer identifiable (Recital 26).

However, the GDPR also introduces a new concept of **pseudonymised data:** data which could be attributed to a natural person by the use of additional information which is kept logically (and securely) separate. Pseudonymised data is still personal data but can, for example, be stored longer for research purposes.

In the 'TELE2 judgement' the CJEU notes that 'the data which providers of electronic communications services must therefore retain…includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular*, to identify* the person with whom a subscriber or registered user has communicated and by what means…'. See paragraph 98 of the judgement (Joint cases C-203/15 and C-698/15).

Based on the above, the GDPR clearly covers this kind of data.

Processing covers any operation or set of operations which are carried out on personal data, and so includes a wide range of activities—from collecting and storing to disclosing and deleting (Art. 4(2)).

The requirements of the GDPR apply to private bodies (this includes companies, NGOs and in most cases also to natural persons) and public bodies (with an exception for police and judicial bodies, which are subject to different rules). However, processing by a natural person in the course of a **purely personal or household activity** is exempt from the scope of the GDPR—(Art. 2(2)(c)). The scope of this household exemption is narrow and the GDPR *does* still apply to controllers and processors which provide the means for processing personal data for such personal or household activities (for example, a company which is running a social media network).

The GDPR also deals with the processing of **special categories of personal data**. These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9). Processing of personal data relating to criminal convictions and offences is also specified (Art. 10). The rules for these special categories of personal data are stricter.

3. Controllers and Processors

Distinguishing between data controllers and data processors is key to understanding the obligations imposed by the GDPR.

A **controller** is defined as a party which (alone or jointly with others) determines the purposes and means of the processing of personal data (Art. 4 (7)). It is the entity that is responsible for what is done with the data and why.

A **processor** is defined as a party which processes personal data on behalf of the controller (Art. 4 (8)). This is usually an organisation providing services to its customer, the data controller.

Different requirements apply to each party, but both have obligations related to security, and confidentiality (Article 28).

4. Data Protection Principles

Underlying the whole Regulation are six key data protection principles, listed in Article 5. These state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner ('**lawfulness, fairness and transparency**' - Art. 5(1)(a));
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**' - Art. 5(1)(b));
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**' - Art. 5(1)(c));
- Accurate and, where necessary, kept up to date ('**accuracy**' - Art. 5(1)(d));
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed ('**storage limitation**' - Art. 5(1)(e)); and
- Processed in a manner that ensures appropriate security of the personal data ('**integrity and confidentiality**' - Art. 5(1)(f)).

A controller is responsible for and should be able to demonstrate compliance with these principles ('**accountability**' - Art. 5(2)).

5. Transparency

Transparency as a key principle of data protection is specified in several GDPR provisions.

Irrespective of the particular legal basis, there is a requirement to provide the data subject with information about the data processing at the time the personal data are collected (i.e. **notice**). This includes the identity and contact details of the controller, the purposes of and legal basis for the processing, details of the data subject's right to withdraw consent (if applicable) and their other rights (see below) (Art. 13(1) and (2)).

In addition to this, the controller shall also provide **information on the legitimate interest** pursued by the controller or by a third party (Art. 13(1) (d)).

The principle of transparency requires that any information addressed to the public or to the data subject must be concise, easily accessible and easy to understand. '*This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for*

*what purpose personal data relating to him or her are being collected, such as in the case of **online advertising**'* (Recital 58).

The principle of transparency also requires that '*the data subject **should be informed of the existence of profiling and the consequences** of such profiling*' (Recital 60).

6. Territorial Scope

The GDPR extends the reach of EU data protection law, and applies to:

- the processing of personal data in the context of an establishment of a controller or processor in the EU (Art. 3(1)). This is regardless of whether the actual processing happens in the EU or not. The concept of establishment implies the '*effective and real exercise of activity through stable arrangements*' (Recital 22).

- the processing of personal data of data subjects who are in the EU, where the processing activities are related to either (a) the offering of goods or services to data subjects in the EU, or (b) the monitoring of data subjects' behaviour, as far as that behaviour takes place within the EU (Art. 3(2)).

Recital 24 states that, **to determine whether data subjects are 'monitored**', it should be determined **whether natural persons are tracked on the internet**. Monitoring includes applying processing techniques which consist of profiling of these persons, particularly with the purposes of taking decisions concerning them or of analysing or predicting their personal preferences, behaviours and attitudes.

When determining whether goods or services are offered to data subjects in the EU, it should be ascertained whether it is apparent that the **controller or processor intends to** offer them in the EU. **Mere accessibility** of a website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is **insufficient** to ascertain such intention (Recital 23).

Where a non-EU controller/processor is subject to the GDPR, the controller or processor is also required to designate **a representative** established in one of the EU Member States where the relevant data subjects are (Art. 27). This obligation does not apply to processing which is occasional and does not include processing of specific categories of data, and is unlikely to result in a risk to the rights and freedoms of natural persons (Art. 27(2)).

7. The Lawfulness of Processing

Processing of personal data can only be carried out if at least one of the legal bases in Article 6 applies. The most relevant GDPR bases to know about for ePR purposes are:

- Where the data subject has given **consent** to the processing of their personal data for one or more specific purposes;
- Where processing is **necessary for the performance of a contract** to which the data subject is party or is necessary to take steps at the request of the data subject prior to entering into a contract;
- Where processing is necessary for compliance with a **legal obligation** to which the controller is subject; and
- Where processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Consent: The GDPR establishes a **high bar** for what constitutes valid consent—it should be provided by a clear, affirmative act and should be freely given, specific, informed and unambiguous (Recital 32).

Ticking a box when visiting an internet website, **choosing technical settings** for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data could be considered valid consent. However, silence, pre-ticked boxes or inactivity are unlikely to constitute valid consent (Recital 32). Language to obtain consent should also be provided in an intelligible and easily accessible form, using clear and plain language (Recital 42).

The requirement of a clear, affirmative act does not require that an individual explicitly consents (although an affirmative act indicating consent may also meet the requirements of 'explicit' consent.) Mere silence or not opting out from a service is not an affirmative act. For consent to be informed, the data subject should be aware of the identity of the controller and the intended purposes of the processing (Recital 42). Freely given consent precludes consent that is given in a situation where there is an imbalance of power. This imbalance often exists in an employment context.

The data subject must have **the right to withdraw their consent** at any time, and it should be as easy to withdraw consent as to give it (Art. 7(2))—this is also essential for demonstrating the consent is 'freely given' (Recital 42). When assessing whether consent is freely given, utmost account shall be taken of whether the provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Art. 7(4) and Recital 43).

Legitimate interest: This basis requires a balancing of, on the one hand, the legitimate interests of a controller or a third party and, on the other hand, the interests and fundamental rights and freedoms of data subjects. Thus, it can be relied on as long as the legitimate interests of the controller or third party are not overridden by the interests, rights and freedoms of a data subject (Recital 47).

In particular, controllers should consider the **data subject's reasonable expectations** at the time of collection, based on the relationship between them and that data subject.

The processing of personal data strictly necessary for the purposes of **preventing fraud** (Recital 47) **and ensuring network and information security** (Recital 49) constitutes a legitimate interest, and the processing of personal data for **direct marketing** purposes may constitute a legitimate interest. '*At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place*' (Recital 47). The legal basis is also closely associated with a right to object (see below).

The GDPR also allows **processing for a purpose other than that for which the personal data have been collected.** However, this is **subject to safeguards** and the processing has to be 'compatible' with the original purpose. In order to establish this, account should be taken of the link between the original purpose and that of the further processing, the context, the relationship with the data subject, the nature of the personal data, the possible consequences and the existence of appropriate safeguards (Art. 6(4)). Where the controller intends to further process the personal data, it shall provide the data subject, prior to that further processing, with information on the purpose and other issues that may be relevant (Art. 13 (3)).

8. Rights of the Data Subject

The GDPR grants various rights to data subjects regarding their personal data, and controllers are required to uphold these. These rights include:

- The right to access their personal data and obtain various other information, such as the purposes of the processing and who the personal data has been disclosed to (Art. 15);
- The right to rectify inaccurate personal data (Art. 16);
- The right to force the controller to erase personal data in certain circumstances—also known as the 'right to be forgotten' (Art. 17);
- The right to data portability, i.e. to receive their personal data in an easily transferable, machine-readable format (Art. 18); and
- **A right 'not to be subject to' a decision based solely on automated processing, including profiling,** which produces legal effects concerning him or her or similarly significantly affects the data subjects (Art. 22).

Furthermore, data subjects have the **right to object** at any time to processing of their personal data based on the controller's legitimate interest. This includes a right to object to any **profiling** based on this legal ground. If this is invoked, the controller cannot continue processing unless they demonstrate 'compelling' legitimate interest grounds which override the interests, rights and freedoms of the data subject (Art. 21(1)).

Where personal data are processed for **direct marketing**, the data subject can object at any time to that processing irrespective of the legal basis relied on (Art. 21(2)). This also includes a

right to object to any **profiling** that is related to that direct marketing, and there is no option for the controller to justify the processing based on their overriding interests (Art. 21(3)).

This right to object should be explicitly brought to the data subject's attention, and presented clearly and separately from any other information (Recital 70).

In 'TELE2', the CJEU notes that the "data [which providers of electronic communications services must retain], taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained…,provides the means…of establishing a profile of the individual concerned.' See paragraph 99 of the judgement (Joint cases C-203/15 and C-698/15).

As per the above, to the extent that data can identify an individual (see paragraph 98 of the judgement) and be used to create a 'profile', Articles 21 or 22 of the GDPR will apply, depending on the effects produced by such profile.

9. Privacy by Design and by Default

The GDPR requires the controller to put in place '*appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation*' (Art. 25(1)). This is known as 'privacy by design and default', and should be implemented both at the time that the controller is determining the means for processing **and** at the time of the processing itself (i.e. from the design stage onwards). Factors such as the 'state of the art', the costs involved and the nature, scope, context and purposes of processing can all be taken into account when assessing what is required for privacy by design.

Recital 78 adds that when developing and designing new data processing applications, the producers of products, services and applications 'should be encouraged' to take data protection into account at the development and design stage, and make sure controllers and processors are able to meet their compliance requirements.

10. Security

The GDPR imposes security obligations on both controllers and processors. Again, taking into account the state of the art, the costs involved and the nature, scope, context and purposes of processing, the controller and processor must implement appropriate technical and organisational measures 'to ensure a level of security appropriate to the risk' (Art. 32(1)). The GDPR states that these include (as appropriate) **pseudonymisation and encryption, measures to ensure confidentiality**, the ability to recover personal data in the event of an incident and processes to test the security measures.

Data breach notification: The GDPR defines a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art. 4(12)). If a data breach occurs, the controller has an obligation to

notify its competent data protection authority unless that breach is unlikely to result in a risk to the rights and freedoms of natural persons (Art. 33(1)). This must be done not later than 72 hours after the controller becomes aware of the breach. If the breach is likely to result in a **high** risk to the rights and freedoms of natural persons, the controller must also communicate the breach to the data subjects without undue delay (Art. 34(1)). A processor must notify the controller without undue delay after becoming aware of a data breach (Art. 33(2)).

11. Risk-based Approach

The GDPR encourages organisations to take a 'risk-based approach' to data protection—i.e. to adapt the measures they implement based on the risk level of the processing. This concept runs throughout the GDPR and underpins many of the Regulation's key obligations. It is an essential element of the principle of accountability (of Art 5(2) and Art. 24 GDPR).

Specifically, controllers must take into account '*the risks of varying likelihood and severity for the rights and freedoms of natural persons*' in the following situations:

- When implementing appropriate technical and organisational measures to ensure and demonstrate that processing is carried out in accordance with the GDPR, i.e. accountability (Art. 24(1));
- When implementing privacy by design and default measures, as described above (Art. 25(1)); and
- When assessing the appropriate level of security measures, taking account in particular of the risks presented by the processing from '*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*' (Art. 32(1) and (2)).

In introducing the concept of pseudonymised data and allowing this to be kept for longer periods under the storage limitation principle, the GDPR also recognises that processing pseudonymised data is a lower risk activity.

12. Data Protection Impact Assessment

When the processing is likely to result in a **high risk,** the controller shall carry out a data protection impact assessment to evaluate, in particular, 'the origin, nature, particularity and severity of that risk'. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken to demonstrate compliance with the GDPR.

Only where the impact assessment indicates that the processing involves a high risk, which the *controller cannot mitigate* by appropriate measures in terms of available technology and costs of implementation, shall a consultation with the supervisory authority take place (Recital 84).

13. Supervisory Authorities

The GDPR preserves the existing supervisory authorities for data protection, but introduces the concept of the ‘lead supervisory authority’, which allows organisations to deal with only one authority when carrying out cross-border processing (i.e. processing personal data of data subjects in multiple Member States). This lead authority (also known as the ‘one-stop-stop’) will be the authority in the EU country where the organisation has its ‘main’ or ‘single' establishment. The lead authority must then cooperate with the other supervisory authorities concerned with the processing under a consistency mechanism (Art. 60), with the ability to refer matters to the European Data Protection Board as necessary.

14. Remedies

The GDPR offers a number of remedies for data subjects in connection with GDPR violations.. The details of these will largely be addressed in Member States’ national laws:

- Data subjects have the right to lodge a complaint with their supervisory authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement (Art. 77);
- Data subjects must also have the right to an effective judicial remedy against a controller or processor (Art. 79); and
- Data subjects have the right to mandate a not-for-profit organisation in certain circumstances to exercise the data subject’s rights on their behalf (i.e. a potential ‘class action’) (Art. 80).

15. Sanctions

The GDPR contains a number of remedial sanctions for breaches of data protection law. They are included in Art. 58 (2) and range from simple warnings to supervisory authorities’ imposing a temporary or definitive ban on processing.

In addition, the GDPR introduced administrative fines. The maximum thresholds for administrative fines which supervisory authorities can award as penalties for breaching the Regulation are laid down in the GDPR and can reach up to 20 million EUR or 4 % of the organisation’s worldwide annual turnover of the preceding financial year (whichever is higher) (Art. 83(5)).

Art. 83(2) sets out a number of factors that should be considered when deciding whether to impose a fine and what amount it should be, including: the nature, gravity and duration of the infringement; the number of data subjects affected; whether the infringement was intentional; any mitigating action taken by the controller or processor; and the level of security and other technical and organisational measures implemented.

ANNEX – Most Relevant GDPR provisions

Recital 4	The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. **This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties,** in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.
Recital 14	The protection afforded by this 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.
Recital 15	In order to prevent creating a serious risk of circumvention, the protection of natural persons should be **technologically neutral** and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.
Recital 18	This Regulation does not apply to the processing of personal data by a natural person in the course of a purely **personal or household activity** and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.
Recital 23	In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. **In order to determine whether such a controller or processor is offering goods or services to data subjects** who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to the data subjects in one or more Member States in the Union. **Whereas the mere accessibility** of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, **is insufficient** to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to the data subjects in the Union.

Recital 24	The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the **monitoring of the behaviour of such data subjects** in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
Recital 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.
Recital 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.
Recital 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.
Recital 40	In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other **legitimate basis,** laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Recital 42	Where processing is based on the data subject's **consent,** the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or **withdraw** consent without detriment.
Recital 43	In order to ensure that **consent is freely given,** consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
Recital 47	**The legitimate interests** of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of **preventing fraud** also constitutes a legitimate interest of the data controller concerned. The processing of personal data for **direct marketing** purposes may be regarded as carried out for a legitimate interest.
Recital 49	The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring **network and information security,** i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Recital 58	**The principle of transparency** requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.
Recital 60	**The principles of fair and transparent processing** require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, **the data subject should be informed of the existence of profiling and the consequences of such profiling.** Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.
Recital 70	Where personal data are processed for the purposes of **direct marketing,** the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.
Recital 78	The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the **principles of data protection by design and data protection by default.** Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Recital 84	In order to enhance compliance with this Regulation where processing operations are likely to result in a **high risk** to the rights and freedoms of natural persons, **the controller should** be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.
Article 2 Material Scope	1. This Regulation does not apply to the processing of personal data: ... (c) by a natural person in the course of a purely personal or household activity;
Article 3 Territorial Scope	1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
Article 4 Definition	**'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; **'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; **'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; **'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; **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; '**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.

	'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; '**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;
Article 5 Principles relating to processing of personal data	1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency'**); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation')**; (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy'**); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation')**; (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**'). 2. The controller shall be responsible for, and able to demonstrate compliance with, paragraph 1 (**'accountability'**).
Article 6 Lawfulness of processing	1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has **given consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their task. 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a

	necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 (1), the controller shall, in order to ascertain whether processing for another **purpose is compatible** with the purpose for which the personal data are initially collected, take into account, inter alia: (a) Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) The nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) The possible consequences of the intended further processing for data subjects; (e) The existence of appropriate safeguards, which may include encryption or pseudonymisation.
Article 7 Conditions for consent	1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the **right to withdraw** his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
Article 13 Information to be provided where personal data are collected from the data subject	1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) The identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the **legitimate interests** pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing. (a) **The period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period; (b) The existence of the right to request from the controller access to and rectification or erasure of personal data or restrictions of processing concerning the data subject or to object to processing as

	well as the right to data portability; (c) Where the processing is based on point (a) of Article 6 (1) or point (a) of Article 9(2), the existence of the right to **withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal; … 3. Where the controller intends to **further process** the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
Article 21 Right to object	1. The data subject shall have **the right to object,** on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including **profiling** based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. 2. Where personal data are processed for **direct marketing purposes**, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. 3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. 4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. 5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
Article 22 Automated individual decision-making, including profiling	1. The data subject shall have the **right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects** him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 25 Data protection by design and by default	1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.
Article 27 Representatives of controllers or processors not established in the Union	1. Where Article 3(2) applies, the controller or the processor shall designate in writing **a** representative in the Union. 2. This obligation shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body. 3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored. 4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation. 5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 32 Security of processing	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to **ensure the ongoing confidentiality,** integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.
Article 33 Notification of a personal data breach to the supervisory authority	1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 Notification of a personal data breach to the data subject	1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3). 3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. 4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.
Article 35 Data protection impact assessment	1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
Article 80 Representation of data subject	1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law. 2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.