GDPR: A Guide to the Regulations

Produced by Arthur Cox, Lex Mundi member firm for Ireland and Northern Ireland.

Please contact associate, Olivia Mullooly at olivia.mullooly@arthurcox.com for more information.

What Data Is Protected?

The **GDPR** regulates the processing of personal data of a living person, which is in the possession or under the control of a data controller.

The **GDPR** is directly effective in all EU Member States without the need for further national legislation. However, the **GDPR** has specific areas in which Member States are either permitted or required to enact national legislation to give effect to its provisions, for example, in relation to the procedure for imposing an administrative fine; the processing of special categories of personal data; the age of consent for processing personal data in the context of online services; and the restrictions and limitations on the application and exercise of data subject rights.

*For detailed information on how these aspects of **GDPR** are enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Personal data is defined as information from which the individual concerned can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The **GDPR** does not apply however to fully anonymized or aggregated data where a living individual cannot be identified.

“Special categories of personal data” is any data that relates to a data subject's:

- Trade union membership.
- Data concerning physical or mental health or condition, or sexual life or orientation.
- Genetic data, biometric data.
- Racial or ethnic origin, political opinions, religious or philosophical beliefs, and which attract a greater level of protection under the **GDPR**.

Data relating to criminal convictions or offenses is subject to specific protection under the **GDPR** and may only be processed under the control of official authority or where authorized by Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Who Is Subject to Privacy Obligations?

The **GDPR** applies to any person or entity that falls within the definition of a data controller or data processor. The **GDPR**'s obligations primarily apply to data controllers, defined as the entity that determines the purposes and means of data processing (alone or together with others).

- A data controller or data processor can be any natural person, corporate entity or other legal person, public authority, agency or other body.
- A data processor is an entity that processes personal data on behalf of the data controller. Data processors will also be subject to certain direct obligations under the **GDPR**.

The **GDPR** applies to:

- the processing of personal data in the context of the activities of a data controller's or data processor's establishment in the EU (regardless of whether the data is processed in the EU or not or regardless of whether the data relates to EU residents or not). (An establishment is not defined but the recitals indicate it will extend to any stable arrangement in a Member State through which the data controller or data processor carries on the relevant activity).

- The processing of personal data of persons within the EU by data controllers or data processors who are established outside the EU, where the processing is related to:
  (a) the offering of goods or services to such data subjects in the EU (irrespective of whether payment is required); or
  (b) the monitoring of the behavior of such data subjects as far as the behavior takes place in the EU.

How Is the Collection of Personal Data Regulated?

The **GDPR** generally requires information to be collected fairly and for a specific purpose and that it only be processed by reference to specific legal grounds.

Under the **GDPR**, a data controller must comply with the following principles under *Article 5*:

- **Lawfulness, fairness and transparency** - the data or, as the case may be, the information constituting the data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- **Accuracy** - the data shall be accurate and, where necessary, kept up to date;
- **Purpose Limitation** - the data—
  - shall have been collected only for specified, explicit and legitimate purposes;
  - shall not be further processed in a manner incompatible with that purpose or those purposes.
- **Data Minimization** – the data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed or are further processed;
- **Storage Limitation** – the data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed;
- **Integrity and Confidentiality** – the data shall be 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 organizational measures; and
- **Accountability** – The data controller shall be responsible for and be able to demonstrate compliance with the principles set out in *Article 5*.

How Are the Use and Disclosure of Personal Data Regulated?

Generally, under the **GDPR**, data controllers are under an obligation to process personal data lawfully, fairly and in a transparent manner (e.g. pursuant to a privacy policy that meets the requirements of the **GDPR**) and for a specified purpose in ways that are compatible with that purpose.

The **GDPR** also requires that all data processing be supported by reference to one or more "lawful bases of processing", which include the following:

Consent

Personal data may be processed based on the data subject's specific, freely given and informed consent. The **GDPR** has prescribed the conditions for obtaining a valid consent which are that:

- such consent must be provided by way of "a statement or by a clear affirmative action" (pre-ticked boxes and implied consent fall short of the standard);
- consent must be fully informed.
- Data subjects have the right to withdraw their consent at any time and in an easy manner.
- Requests for consent must be specifically presented (e.g. consent wording contained within various other terms and conditions would not be valid).

The controller is under an obligation to demonstrate the data subject's consent to the processing where it is the lawful basis.

Legitimate Interests

A data controller may process personal data based on their legitimate interests or those of a third party, (including, for example, advertising or marketing purposes where consent is not otherwise required by law).

The data controller must however inform the data subject of the particular legitimate interest pursued and the data subject has the right to object to the legitimate interest-based processing on grounds particular to his or her situation (see *Right of Objection* below). Public authorities may not rely on this ground.

Contractual Necessity

Personal data may be processed where it is necessary for the performance of a contract to which the data subject is a party to or in order to take steps at the request of the data subject prior to entering the contract. The processing must however be necessary to contract performance rather than merely facilitative.

Legal Obligations

A data controller may process personal data where it is necessary to comply with legal obligations that are imposed on them.

Vital Interest of the Data Subject

The data controller may process personal data where it is necessary to protect the vital interests of the data subject or another natural person.

Public Interest or in the exercise of Official Authority

The data controller may process personal data where it is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller.

Special Categories of Personal Data

The processing of special categories of personal data is subject to separate grounds for processing, which are set out in *Article 9*. These are:

Explicit Consent

See above 'Consent' for an explanation of the requirements for a valid consent. The data subject must be explicitly informed of the request for consent to the processing of special categories of personal data. This ground shall not apply where EU or Member State law prohibits such processing on the basis of explicit consent.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Employment and Social Security and Social Protection Laws

Processing that is necessary for compliance with obligations or exercising rights under employment and social security and social protection laws, as set out in EU or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the rights and freedoms of data subjects

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Vital Interest of the Data Subject

Protection of the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent

Political, Philosophical, Religious or Trade Union Bodies

Processing by a political, philosophical, religious or trade union body or association of the personal data of its members and contacts in the course of its legitimate activities where the personal data is not disclosed outside that body without the consent of the data subjects

Personal Data Publicized by the Data Subject

Personal data that is manifestly made public by the data subject.

Legal Claims

Processing necessary for the establishment, exercise or defense of a legal claim or whenever courts are acting in their judicial capacity;

Substantial Public Interest

Processing necessary for reasons of substantial public interest on the basis of EU or Member State law which is proportionate, respect the essence of the right to data protection and provides for suitable and specific measures to safeguard the rights and interests of the data subjects.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Healthcare & Occupational Health

Processing necessary for the purposes of preventative or occupational medicine, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or pursuant to a contract with a health professional.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Public Health

Processing necessary for reasons of public interest in the area of public health on the basis of EU or Member State law.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Archival, Scientific or Historical Research or Statistical Purposes

Processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of EU or Member State law.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Member State Discretion on Processing of Health Data

Member States may have further conditions with regard to the processing of genetic data, biometric data or data concerning health.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Risk Based Approach

Data controllers must also have "*appropriate technical and organizational measures*" in place to ensure and to be able to demonstrate that processing is performed in accordance with the **GDPR**, taking a risk-based approach (*Article 24*). This requires that the controller takes account of the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The measures must be reviewed and updated where necessary and shall include the implementation of appropriate data protection policies.

Privacy by Design and Privacy by Default

The **GDPR** also introduces new concepts of 'privacy by design' and 'privacy by default' under *Article 25*. This requires that a controller shall implement appropriate technical and organizational 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: and
- the period of their storage and their accessibility.

How Are Storage, Security and Retention of Personal Data Regulated?

The **GDPR** requires that "*appropriate technical and organizational measures*" are in place to protect the security of personal data and that personal data not be retained for longer than is necessary for the purpose or purposes for which the data are processed.

Article 32 provides some detail on the standards that controllers and processors should take account of in determining appropriate security measures against unauthorized or unlawful processing, accidental damage, destruction or loss of data. The data controller must take into account:

- the state of the art;
- the cost of implementing the measures;
- the nature, scope, context and purposes of processing; and
- the risk of varying likelihood and severity for rights and freedoms of the data subject posed by the processing in particular those presented against unauthorized or unlawful processing, accidental damage, destruction or loss of data.

The **GDPR** states that pseudonymization and encryption be considered where appropriate and that controllers maintain system resilience and security testing, back up, recovery and continuity measures.

Data controllers and data processors must ensure all of their employees comply with the security measures in place and not process personal data other than on the instructions of the controller.

Personal data may not be kept for longer than is necessary for the specified purpose or purposes for which it was collected and a data retention procedure or policy should be implemented in this respect.

Are There Rights Exercisable by Data Subjects in Respect of Their Personal Data?

Yes – under the **GDPR**, data subjects have enhanced rights in relation to their personal data, most of which only apply in specific circumstances. These include the retention of the rights of access, deletion (e.g. where processing is unlawful or excessive) and to rectification of inaccurate personal data.

Right of Access

An individual can write to a data controller for a copy of his or her personal data being processed by the data controller. The controller must furnish this within one month of receipt of the request, which period may be extended by two further months where necessary, taking account of the complexity and number of requests. For any further copies requested, the data controller may charge a "reasonable fee based on administrative costs".

The data subject also has the benefit of the following other rights introduced by the **GDPR** which apply in certain circumstances:

Right of Restriction

The right to restrict (i.e. suspend) the processing such as where the accuracy of the data is being contested, the processing is unlawful or the data subject has objected to the processing.

Data Portability

The right to data portability of personal data provided by the data subject to the controller (on the basis of consent or contractual necessity) from one controller to another.

Right of Objection

The right to object to the processing of the personal data where the lawful basis is:

- processing that 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; or
- processing is necessary for the legitimate interests of the controller or a third party.

Processing must be restricted until such time as the controller has demonstrated that its legitimate interest is sufficiently compelling so that it overrides the interests of the data subject. If the controller is unable to do so, then it must cease the processing unless it is necessary for the establishment, exercise or defense of legal claims.

Automated Decisions with Legal or Significant Effects

Data subjects have a right not to be subject to automated decision-making in respect of the personal data, including profiling, with no human intervention where such decision produces legal effects concerning the data subject or similarly significantly affects him or her (e.g. creditworthiness check or e-recruitment). This does not apply where explicit consent is provided, the processing is authorized by EU or Member State law or the processing is necessary for the purposes of entering into or performing a contract with the data subject.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Pursuant to *Article 23* of the **GDPR**, these data subject rights may be subject to limitations or restrictions as prescribed by Member State law where necessary and proportionate to safeguard various matters specified in *Article 23* ranging from issues of national security to the enforcement of civil law claims.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

Are There Restrictions on Cross-Border Data Transfers?

The **GDPR** also restricts the transfer of personal data to a country outside the European Union unless certain conditions or safeguards are in place.

Transfer to Approved Countries Outside the EEA

Transfers of data to a third country or international organisation is permitted where the European Commission has taken an adequacy decision under *Article 45* of the **GDPR** that there is an adequate level of protection of personal data in that country or organisation (including those in the EEA).

The existing list of countries that have previously been approved by the EU Commission will remain in force. Transfers of personal data to the following countries can take place without too much concern:

- Switzerland
- Guernsey
- Argentina
- The Isle of Man
- Faroe Islands
- Jersey
- Andorra

- Israel
- New Zealand
- Uruguay
- Canada (for certain types of personal data pursuant to the *Canadian Personal Information Protection and Electronic Documents Act 2000*)

Transfer to Non-Approved Countries

Where the country to which the personal data will be transferred does not appear on an approved list of countries, the transfer of personal data can still take place only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies are available.

The appropriate safeguards may be provided for by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with *Article 47*;
- so-called model contractual clauses (these clauses contain EU-approved data protection provisions, which incorporate the EU standards into the contract. They can be used where there is no arrangement (such as the *EU-US Privacy Shield*) in place.);
- an approved code of conduct pursuant to *Article 40* together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards; or
- an approved certification mechanism pursuant to *Article 42* together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.
- Using the binding corporate rules

Multinational companies must draft these guidelines in accordance with the requirements of *Article 57* of the **GDPR** and submit them to the competent supervisory authority (i.e. the data protection regulator who is competent under *Article 55 or 56* of the **GDPR**) for approval. They are internal rules that apply to international transfers of data. When they are adhered to, they ensure that the company complies with applicable data protection law.

Are There Any Notification Requirements for Data Breaches?

The **GDPR** introduces a compulsory requirement for controllers to report data breaches to its supervisory authority (i.e. in Ireland, the Data Protection Commission) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to data subjects.

A risk assessment will therefore need to be taken by the controller in evaluating whether the obligation to report arises. Where a breach poses a high risk to data subjects, the **GDPR** also requires that the controller communicate the breach to the affected data subjects without undue delay. Regardless of whether a notification to the regulator is made or not, controllers must document all personal data breaches, comprising the facts, its effects and remedial action taken.

Where a processor has suffered a personal data breach, the processor must notify the controller "without undue delay" after becoming aware of the breach.

Providers of publicly available electronic communications services in public communications networks in Ireland (and where relevant in the EU), are subject to a mandatory reporting obligation in accordance with *EU Regulation No 611/2013*.

Who Is the Privacy Regulator with Competence Over Controllers and Processors in the EU?

Supervisory Authority

Article 55 provides that each supervisory authority has competence to act in relation to matters in its territory.

Lead Supervisory Authority

In circumstances where a controller or a processor is engaged in "cross border processing" (being processing in establishments of that controller or processor in more than one Member State or processing which substantially affects or is likely to substantially affect data subjects in more than one Member State), then the supervisory authority of the main establishment of the controller or processor shall have competence to act in respect of such cross-border processing.

Tasks and Powers of a Supervisory Authority

The **GDPR** provides for enhanced, wide-ranging powers of enforcement to supervisory authorities, who may impose substantial fines for breaches of the **GDPR**.

The tasks of a supervisory authority are set out in *Article 57* of the **GDPR** and include:

- monitoring and enforcing the application of the **GDPR**;
- promoting awareness;
- handling complaints;
- conducting investigations;
- co-operating with other supervisory authorities;
- administrative tasks such as drawing up codes of conduct, reviewing certifications and approving standard contractual clauses for transfers of personal data outside the EEA.

The powers of a supervisory authority are set out in *Article 58* and include:

- ordering the production of information from controllers and processors;
- conducting audits including onsite "dawn raid" type investigations;
- issuing warnings, reprimands, enforcement orders,
- ordering the suspension or ban of non-compliant processing activities;
- imposition of administrative fines and/or commencement or otherwise engaging in legal enforcement proceedings; and
- advisory powers, for example in relation to high risk processing or advising the national legislature on matters relating to data protection.

Administrative Fines

The imposition of administrative fines by a supervisory authority is subject to appropriate procedural safeguards in accordance with Union or Member State law and therefore the mechanism and procedure for imposing a fine may vary from Member State to Member State.

*For detailed information on how this aspect of **GDPR** is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.*

The level of administrative fines are set out in *Article 83* together with examples of aggravating and mitigating factors in determining whether to impose a fine and if so, the level of such fine. In each case, the supervisory authority is to ensure that the imposition of fines is effective, proportionate and

dissuasive. The amount of a fine depends on the nature of the infringement in question with the applicable thresholds being up to:

- 2% of the total global annual turnover of an undertaking for the preceding financial year or EUR10,000,000, whichever is higher; or
- 4% of the total global annual turnover of an undertaking for the preceding financial year or EUR20,000,000, whichever is higher.

How Is Electronic Marketing Regulated?

Direct marketing to individuals is currently regulated at a Member State level under national legislation that gives effect to the *e-Privacy Directive* (**Directive 2002/58/EC**).

The use of publicly available electronic communications services to send unsolicited communications or to make unsolicited calls for the purpose of direct marketing is restricted. Generally, such communications by electronic means require consent or are subject to a right to opt out.

It should be noted that in January 2017, the European Commission published its proposal for an *e-Privacy Regulation*, which will replace the existing *e-Privacy Directive* and may have a broader reach than the current *e-Privacy Directive* in extending to online behavioral advertising. It is currently making its way through the EU legislative process and, subject to conclusion of negotiations on a final draft, is expected to come into force in early 2020.

For detailed information on how this aspect of the e-Privacy Directive is enacted in a particular jurisdiction please contact the Lex Mundi member firm for that jurisdiction directly.