August 2017

Citizens **Information** Board
information · advice · advocacy

Volume 44: Issue 8
ISSN 0790-4290

Relate

The journal of developments in social services, policy and legislation in Ireland

Contents

Page No.

General Data Protection Regulation (GDPR)

The regulation of data is necessary in order to balance the protection of the individual's privacy rights with the rights of organisations and governments to collect and use data for business and administrative purposes.

The regulation of data in Europe is known as data protection. The current data protection framework in Ireland was established under the Data Protection Acts 1988 to 2003; the October 2016 issue of *Relate* discussed this legislation in detail. This framework will be replaced in 2018 by a new European-wide framework, called the General Data Protection Regulation (GDPR). The GDPR places an emphasis on transparency, security and accountability by data controllers and processors, while standardising and strengthening the right of European citizens to data privacy.

The GDPR was adopted on 27 April 2016, and following a two-year implementation period, comes into force across the European Union on 25 May 2018. The GDPR is a European regulation, replacing the existing Data Protection Directive 95/46/EC. The GDPR makes many changes to current European data protection law.

The GDPR is a primary piece of legislation but it also provides that individual member states may enact their own legislation to give specific interpretation to the application of some of the provisions of the Regulation. In Ireland, this is contained within the Data Protection Bill 2017.

Organisations involved in data controlling and data processing of personal data

will need to be aware of the provisions of the GDPR and must comply with those provisions from the date the GDPR comes into force. The legislation introduces severe financial penalties for non-compliance.

Types of data

Personal data

Under the current legislation, personal data relates to or can identify a living person either by itself or together with other available information. Examples of personal data include a person's name, phone number, bank details and medical history.

A **data subject** is the individual to which the personal data relates. These definitions will not change under the GDPR.

Organisations that collect or use personal data will continue to be known as **data controllers and data processors.**

Sensitive data

Under the current Irish legislation, sensitive personal data means personal data relating to any of the following:

- The data subject's racial or ethnic origin, their political opinions or their religious or philosophical beliefs
- Whether the data subject is a member of a trade union
- The data subject's physical or mental health or condition or sexual life
- Whether the data subject has committed or allegedly committed any offence
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

Under the GDPR, this type of data will be called 'special category personal data'. The processing of special category data will be prohibited unless the data subject has given their explicit consent before processing begins or the processing is authorised by law, for example, to protect the interests of a data subject, to comply with employment legislation or for reasons of public interest.

Personal data relating to criminal convictions and offences may only be processed under the control of an official authority.

Extra-territorial application

The GDPR will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of individuals in the EU by a controller or processor established outside the EU, where those processing activities relate to offering goods or services to EU citizens or the monitoring of their behaviour. Non-EU organisations processing the personal data of EU citizens will also have to appoint a representative located in the EU.

Data controllers and data processors

Data controllers are defined in the GDPR as persons or organisations that, alone or with others, determine the purpose and means of processing of personal data. Examples of data controllers include medical professionals, banks, government departments, and voluntary organisations. A local hairdresser or supermarket may be a data controller if that business keeps customer details on file, for example, to make appointments or to operate a promotional points system.

Data processors are persons or organisations that process personal data on behalf of a controller. Examples of data processors include payroll companies and market research companies, all of which may hold or process personal information on behalf of a data controller. The GDPR defines data processing as any operation(s) performed on personal data, for example, collecting, storing, distributing or destroying.

Many controllers also process personal data and do not require a separate data processor.

Profiling

Profiling is a specific form of processing described for the first time under the GDPR. Profiling means any form of automated processing of personal data to evaluate certain personal aspects for any person. For example, the processing of data to analyse or predict a person's performance at work, economic situation, health, personal preferences, interest, behaviour, location or movement.

Controllers and processors who carry out profiling will have to inform data subjects about how the profiling mechanism works before processing.

Data protection principles

Controller principles

The principles of data protection will be stricter under the GDPR. Data controllers will be responsible for these principles and must be able to show that they comply with them.

Personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 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

Processing principles

Data processing under the GDPR will be lawful only if it satisfies one of the defined legal bases.

The legal bases for lawful processing are:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- 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
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 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
- 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. This does not apply to processing by public authorities.

Data subject consent

Where data processing is based on consent, the controller must be able to show that consent was given by the data subject.

If a data subject's consent is given as part of a written document, the request for consent must be presented clearly and separately from any other matters, using plain language. Any part of such a document that conflicts with the GDPR will not be enforceable.

A data subject will have the right to withdraw their consent at any time. Before giving consent, the data subject must be informed of their right to withdraw their consent and it must be as easy to withdraw consent as to give it.

Under the GDPR, a data subject must be at least 16 years old to give valid consent. If the data subject is younger than 16, the consent of a guardian will need to be given. Individual member states may set the age for consent as low as 13 years but not younger.

Rights of the data subject

As a data subject, you will have more rights under the GDPR regarding how your data is handled and processed.

Collection of data

Under the GDPR, when your personal data is collected either directly or indirectly from you, the controller should provide you with the following information:

- Identity and contact details of the controller or their EU representative
- Contact details for the data protection officer
- Purpose of the processing intended and its legal basis
- If the legal basis is a "legitimate interest" of the controller, what that interest is
- The intended recipients of the data
- Any intention to transfer the data outside the EU and if so, the data safeguards in that country
- The period for which the data will be stored or the basis for determining that period
- Your right to request access, rectification, erasure, restriction of use, objection of use and data portability
- Your right to lodge a complaint to a supervisory authority
- Whether you must provide your data as part of a statutory or contractual requirement and the consequences of not providing the data
- The existence and logic of any automated decision-making or profiling processes

If the controller intends to process your data for a purpose other than the purpose for which it was collected, the controller must provide you with information about this purpose before processing begins.

Right of access

Both the current Irish legislation and the GDPR provide you with a right to see a copy of any personal data held by a controller about you. If you believe a person or organisation is processing personal data about you, you can request that they tell you whether they are processing this data. If your data is being processed you will be able to request a copy of that data to be sent to you. The controller will be able to charge a reasonable administrative fee for this. Under the current legislation, the fee cannot be more than €6.35.

You are entitled to the following information:

- The purposes of the processing
- The categories of data being held
- The identity of any recipients who may see this data
- The period for which it will be stored
- Your right to lodge a complaint with a supervisory authority
- Where the information was not collected from you, information about the source
- The use of any automated decision-making processing and information about that process
- If the data is being transferred to a country outside the EU, the data safeguards in that country

Right of rectification, restriction and erasure

Both the current Irish legislation and the GDPR provide you with the right to request controllers to rectify inaccurate or incomplete personal data they hold about you.

You currently have a right to restrict a controller from processing your personal data where:

- The accuracy of the data is in question
- The processing of the data is unlawful
- The controller no longer needs the data for the purpose but it is required by you for other reasons
- You have challenged the legal basis for the processing

Once the processing has been restricted, the controller must inform you before that restriction is lifted.

Under the GDPR you will have a strengthened right of erasure. You can request a controller to erase your data and a controller will have an obligation to erase your data if one of the following applies:

- The data is no longer necessary for the purpose it was collected
- You have withdrawn your consent to the processing of your data
- You object to the processing of your data
- There is no lawful basis for the processing
- The data must be erased to comply with law
- The data was collected in relation to the offer of online services

The right of erasure will also include the right to have publicly available personal data erased or as far as technologically possible, removed from public availability.

The GDPR will also give legislative effect to the recently established 'right to be forgotten' procedure. Right to be forgotten is a right to have search engine results that relate to you or to a certain incident concerning you removed from internet search listings once that information is no longer relevant. For example, if an online search for your name turned up a link to a photograph of you that you believe is no longer relevant for the purpose for which it was collected, you can request that the search engine remove that link from their search results. The right to be forgotten is not an absolute right and requests under the procedure are assessed on a case-by-case basis.

The right of erasure will not apply where processing is necessary because of an overriding freedom of expression, legal or public interest.

Right to data portability

The GDPR will introduce the right to data portability. This means you can request and receive personal data that you have previously provided to a controller in a commonly used and machine-readable format. The right also means you can request one controller to transfer your personal data to another controller.

Right to object and automated decision making

The right to object means you have the right to object to the processing of your data at any time, for example to prevent your data being used for marketing purposes, including profiling. The controller must stop processing your data unless the controller can show there are legitimate grounds or legal reasons for such processing that override your interests.

Your right to not be affected by a decision based on automated processing will also be strengthened under the GDPR. Where a decision is to be made about you that will have significant legal effects, you will have the right to avoid any automated decision-making processing, for example, the decision being made by a bank's loan approval software. A controller must provide human intervention in the decision-making process if you request it.

Privacy notices

Data controllers must have appropriate measures to comply with your rights and must provide information to you in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

If a controller does not comply with a request from you, the controller must give you reasons for this and should inform you of your right to make a complaint to the supervisory authority.These rights will not apply where the data can no longer identify you.

Obligations of controllers and processors

Data privacy by design

The GDPR will introduce the concept of privacy by design. This will mean the inclusion of data protection measures from the outset of designing a processing system. The controller must implement appropriate technical and organisational measures in order to meet the requirements of the Regulation and protect the rights of data subjects.

For example, controllers should design their processes so that they collect only the data absolutely necessary for their purposes, and access to personal data should be limited to only those necessary for processing. Controllers may also temporarily anonymise personal data.

Controllers will be able to apply for certification from a supervisory authority, which will demonstrate that their processes are designed to comply with the Regulation.

Relationship between controller and processor

Where processing is to be carried out by a processor and not the controller, the controller must use only those processors who guarantee that their systems of processing meet the requirements of the Regulation.

The controller must have a contract with the processor setting out the scope of the processing required by the controller and the processor's obligations under the Regulation. A processor cannot outsource this processing to another processor without the controller's consent and a similar contract agreed with that second processor.

Processors should follow any relevant code of conduct that may be prepared by a supervisory authority. Processors may also receive certification demonstrating their compliance with the Regulation.

Processing record

Under the GDPR, any controller with more than 250 employees or who processes sensitive information will have to keep a record of the processing activities under their responsibility.

That record will consist of:

- The name and contact details of the controller
- The purposes of the processing
- A description of the categories of data subjects and personal data
- Categories of recipients of the data
- Any transfers of data to third countries and that country's data safeguards
- Time limits for erasure of data
- A description of the data security measures in place

Processors will have to keep similar records. These records can be inspected by the supervisory authority on request.

Security of personal data

Controllers and processors have an obligation to keep personal data secure. Under the GDPR, controllers and processors will have to consider implementing modern security measures appropriate for the risks involved in their activities. For example, risks may come from accidental or unlawful destruction of stored data or unauthorised disclosure, access or alteration.

The security measures may include anonymisation or encryption of data and restoring or backing up stored data. Controllers and processors will need to review and evaluate their security measures to comply with any code of conduct that may be published in the future.

Data breach reporting

Under the GDPR, a controller must notify the supervisory authority of a personal data breach without delay where that breach is a likely to result in a risk to the rights and freedoms of the data subject. Notification should be made within 72 hours of the controller becoming aware of the breach. Data processors will be required to notify the respective controllers if the processor becomes aware of a breach. The controller should also notify the data subject without delay.

Data protection impact assessment

Under the GDPR, when a controller intends to carry out high-risk processing they will have to first carry out a data protection impact assessment. The supervisory authority

will prescribe a list of the kind of processing operations that may be high risk. These processes may include processing using new technology, profiling and automated decision-making processing, processing large amounts of sensitive personal data or systematically monitoring a publicly accessible area.

The data protection impact assessment should include:

- A description of the processing and the purpose
- An assessment of the necessity of the processing
- An assessment of the risks to the rights and freedoms of the data subjects
- The measures to be used to address the risks

The controller may consult with the supervisory authority who may provide advice to the controller.

The controller should carry out a review after the processing has begun to ensure it is being performed in line with the data impact assessment that was carried out.

The controller should also seek the advice of their data protection officer.

Data protection officers

Under the GDPR, data protection officers must be appointed by controllers and processors whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale or of special categories of personal data or data relating to criminal convictions and offences.

Data protection officers (DPOs):

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Must provide contact details to the relevant supervisory authority
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management in their organisation
- Must not carry out any other tasks that could result in a conflict of interest

DPOs must be involved in all issues of data protection and must be given the resources to carry out their tasks. You will be able to contact the DPO of an organisation about any issues relating to your personal data held by that organisation.

The tasks of the DPO will be to:

- Inform and advise their organisation about its data protection obligations
- Monitor their organisation's compliance with the GDPR and any national data protection legislation
- Advise on data protection impact assessments and monitoring performance
- Liaise with the supervisory authority

Codes of conduct and certification

Associations and other bodies representing controllers and processors may prepare codes of practice that will specify how the GDPR should be specifically applied. These bodies must submit their draft codes of conduct to the relevant supervisory authority for approval.

In order to enhance transparency and compliance with this Regulation, the GDPR will introduce certification mechanisms and data protection marks, allowing data subjects to quickly assess the level of data protection of relevant products and services.A list of certified organisations will be publicly available.

Codes of conduct and approved certification mechanisms will also assist controllers in identifying the risks related to their type of processing and in adhering to best practice.

For processors seeking to process information on behalf of controllers, the adherence of a processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.

Transferring data outside the EU

Any transfer of personal data outside the EU or to an international organisation will be strictly regulated under the GDPR. The Regulation will also apply to any onward transfer of personal data from one non-EU member state to another.

Such a transfer of personal data may only take place where the European Commission has decided that the non-EU member state or business sector within that country has an adequate level of data protection in place. In deciding if there is adequate protection, the Commission will look at that country's laws, respect for human rights, the existence of any data protection authority and the international commitments that country has made relating to personal data. After deciding if a country or sector has adequate data protection, the Commission will continue to monitor that country in terms of its data protection practices.

The Commission will publish a list of all such approved countries, sectors and international organisations.
If a controller or processor wants to transfer data to an unapproved country, sector or international organisation, that controller or processor must provide the appropriate safeguards and ensure that any data subjects will still be able to exercise their rights.

Oversight

Independent supervisory authorities

Under the current Irish legislation, the Data Protection Commissioner is responsible for supervising data protection in Ireland. Under the GDPR, each member state will have one or more independent public authorities responsible for monitoring the application of the Regulation. In Ireland, under the Data Protection Bill 2017, the Data Protection Commissioner will be replaced with a Data Protection Commission.

Each supervisory authority will:

- Monitor and the enforce the application of the GDPR
- Promote public awareness of the rules and rights around data processing
- Advise the government on data protection issues
- Promote awareness among controllers and processors of their obligations
- Provide information to individuals about their data protection rights
- Maintain a list of processing operations requiring data protection impact assessment

Each authority will have the power to order any controller or processor to provide information that the authority requires to assess compliance with the Regulation. The authority may carry out investigations of controllers and processors in the form of data audits, including accessing the premises of a controller or processor. The authority can order a controller or processor to change their processes, comply with data subject requests. The authority can also issue warnings to controllers and processors and can ban processing as well as commence legal proceedings against a controller or processor.

European Data Protection Board

The GDPR will introduce a new European data protection supervisory authority. The European Data Protection Board will be responsible for ensuring the GDPR is applied consistently across Europe. The Board will issue guidelines and recommendations on the application of the Regulation. The Board will also advise the EU Commission on the application of the Regulation and any updates that may be required. The Board will be made up of the head of one supervisory authority of each member state and a European Data Protection supervisor.

Penalties

Under the GDPR, organisations in breach of the Regulations can be fined up to 2% of their annual global turnover or €10 million, whichever is greater, for lesser breaches, for example, not having their records in order, not notifying the supervisory authority and data subject about a breach or not conducting impact assessment. For the most serious infringements, for example, not having sufficient customer consent to process data or violating the core of privacy by design concepts, organisations can be fined up to 4% of their annual global turnover or €20 million, whichever is greater.

Penalties will apply to both controllers and processors. Member states may introduce further fines legislation, which will be enforceable within that state only.

General Data Protection Bill 2017

The Department of Justice and Equality is currently preparing the Data Protection Bill 2017. The Bill will transpose the Regulation into national law and will replace the Data Protection Commissioner with a Data Protection Commission with the possibility of up to three Commissioners depending on future workload.

The Bill will also give further effect to the Regulation, for example, it will provide for the imposition of fines on public authorities for breaches of data protection law where such authorities are acting in competition with private operators.

Related legislation

Data Protection Directive for Police and Criminal Justice Authorities

The Data Protection Directive for Police and Criminal Justice Authorities has applied since 5 May 2016. As this legislation is a Directive and not a Regulation, EU member states must introduce national legislation to ensure compliance with the Directive before 6 May 2018.

The Directive specifically regulates the processing of data by police and criminal justice authorities in the EU.
The Directive requires that the data collected by law enforcement authorities is:

The Citizens Information Board provides independent information, advice and advocacy on public and social services through citizensinformation.ie, the Citizens Information Phone Service and the network of Citizens Information Services. It is responsible for the Money Advice and Budgeting Service and provides advocacy services for people with disabilities.

Head Office
Ground Floor
George's Quay House
43 Townsend Street
Dublin 2
D02 VK65

t 0761 07 9000
f 01 605 9099
e info@ciboard.ie
w citizensinformationboard.ie

- Processed lawfully and fairly
- Collected for specified, explicit and legitimate purposes and processed only in line with these purposes
- Adequate, relevant and not excessive in relation to the purpose in which they are processed
- Accurate and updated where necessary
- Kept in a form that allows identification of the individual for no longer than is necessary for the purpose of the processing
- Appropriately secured, including protection against unauthorised or unlawful processing

EU member states must establish time limits for erasing the personal data or for a regular review of the need to store such data.

The Directive requires that the law enforcement authorities make a clear distinction between the data of different categories of persons including:

- Those for whom there are serious grounds to believe they have committed or are about to commit a criminal offence
- Those who have been convicted of a criminal offence
- Victims of criminal offences or persons whom it is reasonably believed could be victims of criminal offences
- Those who are parties to a criminal offence, including potential witnesses

National authorities must implement measures to ensure a level of security for personal data, for example, preventing unauthorised persons access processing equipment; preventing the unauthorised reading, copying, changing or removal of data; and preventing the unauthorised input, viewing, changing or deleting of stored personal data.

The Passenger Name Record Directive

The Passenger Name Record Directive (PNRD) has applied since 21 April 2016. EU member states must introduce national legislation to ensure compliance with the PNRD before 24 May 2018.

The PNRD regulates the use of passenger name records (PNR) data in the EU for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes.

PNR data includes:

- Travel dates
- Travel itinerary
- Ticket information
- Contact details
- Means of payment used
- Baggage information

Each EU member state must establish a Passenger Information Unit (PIU). A PIU is responsible for collecting, storing and processing PNR data, as well as transferring that data or the results of its processing to the competent national authorities. A PIU may exchange PNR data and the results of its processing with other EU member states and Europol.

Airlines must provide PIUs in EU member states with the PNR data for flights entering or departing from the EU. It also allows, but does not require, EU member states to collect PNR data concerning selected internal EU flights.

Data provided by airlines will be stored in a database by a PIU for five years. After six months storage, the PNR data must be de-personalised. The data collected may only be processed to prevent, detect, investigate and prosecute terrorist offences and serious crime.

Data should only be processed in the following cases:

- For a pre-arrival assessment of passengers against pre-determined risk criteria and relevant law enforcement databases
- For use in specific investigations or prosecutions
- As input in the development of risk assessment criteria