General Data Protection Regulation (GDPR) Overview

km security consulting ltd

Prepared by
Kieran Mongan

Nov 2018

Course Objectives

The objectives of today's training are to provide:

- an overview on the General Data Protection Regulation (GDPR);
- specific focused training on Section 39 of the DPA 2018 - Communication with data subjects by political parties, candidates for and holders of certain elective political offices
- specific focused training on Section 40 of the DPA 2018 - Processing of personal data and special categories of personal data by elected representatives; and,
- specific focused training on the Irish County Councils proposed policy and procedures for processing of personal data with regard to their interactions with the AILG elected members.

Overview of the General Data Protection Regulation (GDPR)

The Nature of European Law

Two main types of legislation:

Directives

- Require individual implementation in each Member State
- Implemented by the creation of national laws approved by the parliaments of each Member State
- European Directive 95/46/EC is a directive
- Irish Data Protection Acts (1998 & 2003) are the Irish Implementation of the ED 95/46/EC

Regulations

- Immediately applicable in each Member State
- Require no local implementing legislation
- EU GDPR is a regulation

History of the EU's data protection laws

- **Post WWII,** concerns about protection of human rights
- **1950**, EU Convention on Human Rights (ECHR) introduces privacy
- **1980**, OECD guidelines on trans-border data flows
- **1981**, EU Treaty 108 – eight principles for protecting personal data
  - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - Different Member States implemented their own laws to reflect this
- **1988,** Irish Data Protection Act 1988 established
- **1995**, EU Data Protection Directive (95/46/EC)

  All Member States requested to transpose into law
  - Inconsistent protection of individual rights
  - Uneven organisational playing field
- **1998**, Human Rights Act (HRA 1998) – Article 8 'right to privacy'.
- **2003,** Irish Data Protection (Amendment) Act 2003 established (Data Protection Acts 1988 and 2003)

History of the EU's data protection laws

- **2016**, EU GDPR approved, becomes law two years from publication.
  - On 8 April 2016 the Council adopted the Regulation.
  - On 14 April 2016 the Regulation was adopted by the European Parliament.
  - On 4 May 2016, the official text of the Regulation was published in the EU Official Journal in all the official languages.
  - The Regulation entered into force on 24 May 2016, and applies from **25 May 2018**.
- **2018,** Irish Data Protection Act 2018 published.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

General Provisions

Article 1: Subject-matter and objectives

Natural person = a living individual.

Natural persons have rights associated with:

- The protection of personal data;
- The protection of the processing of personal data;
- The unrestricted movement of personal data within the EU.

Article 2: Material scope

In material scope:

- Personal data that is processed wholly or partly by automated means.
- Personal data that is part of a filing system, or intended to be.

Out of material scope:

- Personal data used in the course of an activity outside of EU law.
- Personal data used in border checks, asylum and immigration status.
- Personal data used in relation to a purely personal activity.
- Personal data used for the purpose of crime prevention, etc.

Article 3: Territorial scope

- The Regulation applies to controllers and processors in the EU irrespective of where processing takes place.
- It applies to processing activities that are related to:
  - Goods or services, irrespective of whether payment is required.
  - The monitoring of data subjects' behaviour within the EU.
- It applies to controllers not in the EU, but where Member State law applies.

General Provisions

Article 4: Definitions

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

General Provisions

Article 4: Definitions

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

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Principles

Article 5: Principles relating to the processing of personal data

The Data Protection principles largely remain the same. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

Introduction of the new requirement that the controller be able to demonstrate “accountability”.

Principles

Article 6: Lawfulness of processing

Processing will only be lawful if ONE of the following conditions is met:

a) Data subject gives consent for one or more specific purposes.

b) Processing is necessary to meet contractual obligations entered into by the data subject.

c) Processing is necessary to comply with legal obligations of the controller.

d) Processing is necessary to protect the vital interests of the data subject or of another natural person.

e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller.

f) Processing is for the purposes of legitimate interests pursued by the controller or 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.

Principles

Article 7: Conditions for consent

The following conditions apply for consent:

- Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subjects' agreement to the processing of personal data.
- Controllers must be able to demonstrate that consent was given.
- Written consent must be clear, intelligible and easily accessible, otherwise not binding.
- Consent can be withdrawn any time, and it must be as easy to withdraw consent as give it.
- Consent to processing data is not necessary for the performance of a contract.
- Consent should be non-disruptive to the use of the service.
- Ticking a box (not pre-ticked) or choosing appropriate technical settings is still valid.

Principles

Article 8: Conditions applicable to child's consent for information society services

The following conditions apply for child consent:

- If consent is given and the child is at least 16 years old.
- Below the age of 16 years, parental authorisation is required.
- Member States may reduce the definition, but not below 13 years.
- Controller shall make reasonable efforts to verify authorisation.
- Rules on the validity, formation or effect of a contract in relation to a child shall not be affected.
- Information Society Services – Google, eBay etc.

Principles

Article 9: Processing of special categories of personal data

Processing of the following types of personal data is prohibited:

- Race;
- Ethnic origin;
- Political opinions;
- Religion;
- Philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Health data;
- Concerning a natural person's sex life;
- Sexual orientation.

Exceptions:

- The data subject has given explicit consent.
- It is necessary to fulfill the obligations of controller or of data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out by a foundation or not-for-profit organisation.
- The personal data has manifestly been made public by the data subject.
- Establishment, exercise or defence of legal claims.
- Reasons of public interest in the area of public health.
- Archiving purposes in the public interest.
- A Member State has varied the definition of a special category.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Information and access to personal data

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

The controller shall provide any information or communication referring to the data subject in a

- concise,
- transparent,
- intelligible and
- easily accessible form;
- using clear and plain language;
- in particular for any information addressed specifically to/in relation to a child.

- The information should be provided in writing, other means or orally (provided the identity of the data subject is proven by other means)

The controller must facilitate the exercise of data subjects' rights.

- 'Data subject access request'.
  - Time period reduced to 1 month from 40 days.
- Fees abolished;
  - Exceptions for excessive or vexatious requests – onus on data controller to prove.

Information and access to personal data

Article 13.1: Information to be provided where personal data collected from the data subject.

When obtaining personal data, the controller shall provide the data subject with all of the following information (privacy notice):

- The identity and contact details of the controller and their representative.
- The contact details of the data protection officer, where applicable.
- The purposes of the processing as well as the legal basis for the processing.
- The legitimate interests pursued by the controller or by a third party.
- The recipients or categories of recipients of the personal data, if any and where applicable.
- The fact that the controller intends to transfer personal data to a third country and the existence of adequacy conditions.

Article 14: And where obtaining personal data other than from the data subject, the controller shall provide (in addition to the above) the data subject with

- From which source the personal data originate, and if applicable, whether it came from publicly accessible sources.
- The categories of personal data concerned.

Information and access to personal data

Article 13.2: When obtaining personal data, the controller shall provide the data subject with the following further information to ensure fair and transparent processing:

- The period of time that the data will be stored.
- The right to rectification, erasure, restriction, objection.
- The right to data portability.
- The right to withdraw consent at any time.
- The right to lodge a complaint with a supervisory authority.
- The consequences of the data subject's failure to provide data.
- The existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject.

Information and access to personal data

Article 15: Right of access by the data subject

The right is subject to fewer conditions and data subjects can request more extensive information concerning:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients to whom the personal data have been or will be disclosed.
- The period for which the personal data will be stored.
- The right to rectification, erasure, restriction or objection.
- The right to lodge a complaint with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their source.

Information and access to personal data

Article 16: Right to rectification

The data subject shall have the right to the rectification of inaccurate personal data:

- right to have incomplete data completed,
- including by means of a supplementary statement.

Information and access to personal data

Article 17: Right to erasure ('right to be forgotten')

Data subjects have the right to the erasure of personal data where one of the following grounds applies:

- The data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws the consent on which the processing is based and where there is no other legal ground for the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data have been unlawfully processed.
- The personal data have to be erased for compliance with a legal obligation.
- The personal data have been collected in relation to the offer of information society services to a child (< 16 years of age).

Information and access to personal data

Article 18: Right to restriction of processing

The data subject shall have the right to restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject.
- The processing is unlawful, and the data subject opposes the erasure of the personal data, and requests the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the original processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims.
- The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Information and access to personal data

Article 20: The right to data portability

The data subject has the right to have personal data transmitted to another data controller.

- The data controller must provide the data subject with a copy of personal data in a structured, commonly used and machine-readable format.
- The data controller must not hinder the transmission of personal data to a new data controller.
- The right of data portability only applies where:
  - data is processed by automated means; and
  - the data subject has provided consent to the processing or the processing is necessary to fulfil a contract; and
  - the data was provided by the data subject.

Information and access to personal data

Article 21: Right to object

The data subject shall have the right to object to:

- Processing for a task in the public interest;
- Processing based on legitimate interests:
  - processing of personal data for direct marketing;
  - processing of data for profiling;
  - processing of data by automated means;
  - processing for scientific or historical purposes.

Exceptions:

- The controller must demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

Information and access to personal data

Article 23: Restrictions

Controllers and processors may, by EU or Member State law, be restricted in applying specific articles where it is a necessary and proportionate measure to safeguard:

- National security,
- Defence,
- Public security.
- All activities related to prosecution of criminal offences.
- Economic or financial interests of the Union or of a Member State, including public health and social security.
- The protection of judicial independence and judicial proceedings.
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.
- A monitoring, inspection or regulatory function connected with the aforementioned activities.
- The protection of the data subject or the rights and freedoms of others.
- The enforcement of civil law claims.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Controller and Processor Obligations

Article 24: Responsibility of controller

- Implement appropriate technical and organisational measures.
- Implement data protection policies.
- Adhere to codes of conduct to demonstrate compliance.

Controller and Processor Obligations

Article 25: Data protection by design and by default

- The controller shall implement appropriate technical and organisational measures.
- Only data necessary for each specific purpose is processed.
- The obligation applies to the following:
  - the amount of data collected;
  - the extent of the processing;
  - the period of storage;
  - the accessibility to that data.
- Personal data may not be made accessible to an indefinite number of natural persons without the individual's intervention.
- Pseudonymisation, Anonymisations, Encryption, Role based access and Minimisation are recognised techniques in data protection by design.

- Risk Management, Patch & Vulnerability Management, Access Management, Data Classification, Vendor Management etc. remain fundamental controls required to protect data

Controller and Processor Obligations

Article 28: Processor

A legal contract must ensure that the processor:

- processes the personal data only on documented instructions from the controller;
- ensures that persons authorised to process the personal data observe confidentiality;
- takes appropriate security measures;
- respects the conditions for engaging another processor;
- assists the controller by implementing appropriate technical and organisational measures;
- assists the controller in ensuring compliance with the obligations in respect of security of processing;
- deletes or returns all the personal data to the controller after the end of the provision of services; and
- makes available to the controller all information necessary to demonstrate compliance with the Regulation.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Security of Personal Data

Article 32: Security of processing

A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:

- Pseudonymisation and encryption of personal data.
- Ensuring the ongoing confidentiality, integrity and availability of systems.
- A process for regularly testing, assessing and evaluating the effectiveness of security measures.
- Taking security measures that comply with the concept of data protection by design.
- Taking steps to ensure that any natural person working for the controller or processor only processes data under explicit instruction unless required to do so by EU or Member State law.

Security of Personal Data

Article 33: Notification of a personal data breach to the supervisory authority

- A "'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".
- Data controllers are obliged to report security breaches to the relevant supervisory authority without undue delay;
- Where feasible, not later than 72 hours after they first become aware.
- If not made within 72 hours, a justification for the delay must be provided.
- Not necessary to notify where breach is "unlikely to result in a risk for the rights and freedoms" of data subjects.
- The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification shall at least:

- describe the nature of the personal data breach, including categories of data, #data subjects, #personal data records;
- communicate the name and contact details of the data protection officer or their representative;
- describe the likely consequences of the personal data breach;
- describe the mitigating measures taken or proposed to be taken by the controller to address the personal data breach.

The controller may provide information in phases and shall document facts of the breach and remediation to a degree that that enables the supervisory authority to verify compliance with this Article.

Security of Personal Data

Article 34: Communication of personal data breach to the data subject

- Where there is 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.
- Communication of the breach to the data subject shall be described in clear and unambiguous terms.
- Breach notification to the data subject is not required if:
  - the personal data has been rendered unintelligible to any person who is not authorised to access it, such as through encryption;
  - the controller has measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
  - 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.

- Supervisory authority may direct controller to notify data subject if it considers personal data breach to be a high risk

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Data Protection Officer

Article 37: Designation of the data protection officer

- DPOs appointed in three situations:
  - Where the processing is carried out by a public body.
  - Where core activities require regular and systematic monitoring of personal data on a large scale.
  - Where core activities involve large-scale processing of special categories of data.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Codes of Conduct and Certification

Article 40: Codes of conduct

- Codes of conduct may be made available at national and European level.
- Compliance with codes of conduct is another method for organisations to demonstrate they have taken steps to implement appropriate policies and procedures.

Article 42: Certification

- The establishment of data protection certification mechanisms:
  - Transfer of personal data to third countries.
  - Certification will be voluntary.
  - Certification does not absolve controller of need to comply.
  - Processing certified for a maximum of three years.
- Possible development of European Union data protection seal.

Article 43: Certification bodies

- Subject to approval by supervisory authorities.
- Must demonstrate independence and expertise.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Independent Supervisory Authorities

Articles 51 –52: Supervisory authority

Member States must provide one or more independent supervisory authorities:

- Monitor the application of the GDPR.
- Supervisory authorities must act independently.
- Member States must provide adequate resources.

Lead supervisory authorities:

- Entities operating in more than one state can choose a lead supervisory authority for all their pan-EU activities.
- Monitor compliance in respect of cross-border processing by an organisation whose main establishment is in that Member State.

Independent Supervisory Authorities

Article 58: Powers

Each supervisory authority:

- shall have investigative powers.
- shall have corrective powers.
- shall have authorisation and advisory powers.
- will have legal power to enforce.
- shall be subject to judicial remedy.
- is not limited by its Member State.

Independent Supervisory Authorities

Article 77: Right to lodge a complaint with a supervisory authority

- Every data subject has the right to launch a complaint with a supervisory authority:
  - Member State of habitual residence;
  - Place of work; or
  - Place of alleged infringement.

The supervisory authority shall inform the complainant of progress, including the possibility of judicial remedy.

GDPR

The GDPR has eleven chapters, 99 articles and 173 recitals:

- **Chapter I General Provisions: Articles 1 –4**
- **Chapter II Principles: Articles 5 –11**
- **Chapter III Rights of the Data Subject: Articles 12 –23**
- **Chapter IV Controller and Processor: Articles 24 –43**
  - Controller and Processor Obligations
  - Security of Personal Data
  - Privacy Impact Assessments
  - Data Protection Officer
  - Codes of Conduct
- **Chapter V Transfer of Personal Data to Third Countries: Articles 44 –50**
- **Chapter VI Independent Supervisory Authorities: Articles 51 –59**
- Chapter VII Cooperation and Consistency: Articles 60 –76
- **Chapter VIII Remedies, Liabilities and Penalties: Articles 77 –84**
- Chapters IX –XI Various specific provisions: Articles 85 –99

Remedies, Liabilities and Penalties

Article 77: Right to lodge a complaint with a supervisory authority

- Every data subject has the right to launch a complaint with a supervisory authority:
  - Member State of habitual residence;
  - Place of work; or
  - Place of alleged infringement.

- The supervisory authority shall inform the complainant of progress, including the possibility of judicial remedy.

Article 79: Right to an effective judicial remedy against a controller or processor.

- Right to judicial remedy where their rights have been infringed as a result of the processing of personal data.
- Proceedings shall be brought before the courts of the Member State where the controller or processor has an establishment.
  - May alternatively be brought before the courts of the Member State where the data subject habitually resides.

Remedies, Liabilities and Penalties

Article 82: Right to compensation and liability.

- Any person who has suffered material or non-material damage shall have the right to receive compensation from the controller or processor.
- The controller shall be liable for damage caused by processing.
- The processor is liable only for damage caused by processing or where it has acted contrary to lawful instructions of the controller.
- Joint and several liability to ensure effective compensation.
- Compensation clawback provision.

Remedies, Liabilities and Penalties

Article 83: General conditions for imposing administrative fines.

- Imposition of administrative fines will in each case be ***effective, proportionate, and dissuasive.***

Must take account of:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them;
- any relevant previous infringements;
- the degree of cooperation;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known;
- where corrective powers have previously been ordered against the controller or processor;
- adherence to approved codes of conduct or approved certification mechanisms;
- and any other aggravating or mitigating factors.

Remedies, Liabilities and Penalties

Article 83: General conditions for imposing administrative fines.

€10,000,000 or, in case of an undertaking, 2% total worldwide annual turnover in the preceding financial year (whichever is greater).

Articles:

8: Child's consent 11: Processing not requiring identification 25: Data protection by design and by default 26: Joint controllers 27: Representatives of controllers not established in EU 26 –29 and 30: Processing 31: Cooperation with the supervisory authority 32: Data security	33: Notification of breaches to supervisory authority 34: Communication of breaches to data subjects 35: Data protection impact assessment 36: Prior consultation 37 –39: DPOs 41(4): Monitoring approved codes of conduct 42: Certification 43: Certification bodies

Remedies, Liabilities and Penalties

Article 83: General conditions for imposing administrative fines.

€20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher).

Articles:

5: Principles relating to the processing of personal data 6: Lawfulness of processing 7: Conditions for consent 9: Processing special categories of personal data (i.e. sensitive personal data) 12 –22: Data subject rights to information, access, rectification, erasure, restriction of processing, data portability, object, profiling	44 –49: Transfers to third countries 58(1): Requirement to provide access to supervisory authority 58(2): Orders/limitations on processing or the suspension of data flows

Power of Commission to decide to impose administrative fine: General

141. (1) The Commission, in considering—

(a) whether to make a decision to impose an administrative fine, and

(b) where applicable, the amount of such a fine,

shall act in accordance with this section and Article 83.

(2) Where a controller to whom *section 111(2)(b)*, *112(2)(b)* or *133(9)* applies is a controller by virtue of his or her being the subject of a designation under *subsection (1)* or *(2)* of *section 3*, a decision by the Commission to impose an administrative fine in respect of the infringement or failure concerned shall be a decision to impose an administrative fine on the appropriate authority that, or, as the case may be, the Minister who, made the designation, and not on the controller.

(3) Where *subsection (2)* applies, a reference in *sections 115(1)(a)*, *133(9)(b)* and this Chapter to a controller shall be construed as a reference to the appropriate authority or Minister concerned.

(4) Where the Commission decides to impose an administrative fine on a controller or processor that—

(a) is a public authority or a public body, but

(b) is not a public authority or a public body that acts as an undertaking within the meaning of the Competition Act 2002, the amount of the administrative fine concerned shall not exceed €1,000,000.

Going to take a short break

Agenda:

- Provide overview training to AILG elected members on GDPR;
- Provide specific focused training on Section 39 of the Data Protection Act 2018 - Communication with data subjects by political parties, candidates for and holders of certain elective political offices
- Provide specific focused training on Section 40 of the Data Protection Act 2018 - Processing of personal data and special categories of personal data by elected representatives; and,
- Provide specific focused training on the Irish County Councils proposed policy and procedures for processing of personal data with regard to their interactions with the AILG elected members.

Section 39 of the Data Protection Act 2018 - Communication with data subjects by political parties, candidates for and holders of certain elective political offices

Section 39

Communication with data subjects by political parties, candidates for and holders of certain elective political offices

(1) A specified person may, in the course of that person's electoral activities in the State, use the personal data of a data subject for the purpose of communicating in writing (including by way of newsletter or circular) with the data subject.

(2) Communicating in accordance with *subsection (1)* shall, for the purposes of Article 6(1)(e), be considered to be the performance of a task carried out in the public interest.

(3) In this section, "specified person" means—

(a) a political party,

(b) a member of either House of the Oireachtas, the European Parliament or a local authority, or

(c) a candidate for election to the office of President of Ireland or for membership of either House of the Oireachtas, the European Parliament or a local authority.

(4) In this section and in *sections 48*, *58* and *59*, "electoral activities" includes the dissemination of information, including information as to a person's activities and policies, that might reasonably be of interest to electors.

Coimisiún Cosanta Sonraí
Data Protection Commission

Guidance available to Elected Representa-tives on the DPC web-site

Elections and Canvassing: Data Protection and Electronic Marketing

Ireland is a democracy and politicians must be able to effectively communicate with voters

Coimisiún Cosanta Sonraí Data Protection Commission

Principles of Data Protection

As a data controller, you should ensure that at all times your use of the constituent information you process complies with the principles relating to the processing of personal data. Processing means doing anything with personal data including holding it in a database or any other form. This means you should always:

1. **Process it lawfully, fairly, and in a transparent manner;**
2. **Collect it only for one or more specified, explicit and legitimate purposes, and do not otherwise use it in a way that is incompatible with those purposes;**
3. **Ensure it is adequate, relevant and limited to what is necessary for the purpose it is processed;**
4. **Keep it accurate and up-to-date and erase or rectify any inaccurate data without delay;**
5. **Where it is kept in a way that allows you to identify who the data is about, retain it for no longer than is necessary;**
6. **Keep it secure by using appropriate technical and/or organisational security measures;**
7. **Be able to demonstrate your compliance with the above principles; and**
8. **Respond to requests by individuals seeking to exercise their data protection rights (for example the right of access).**

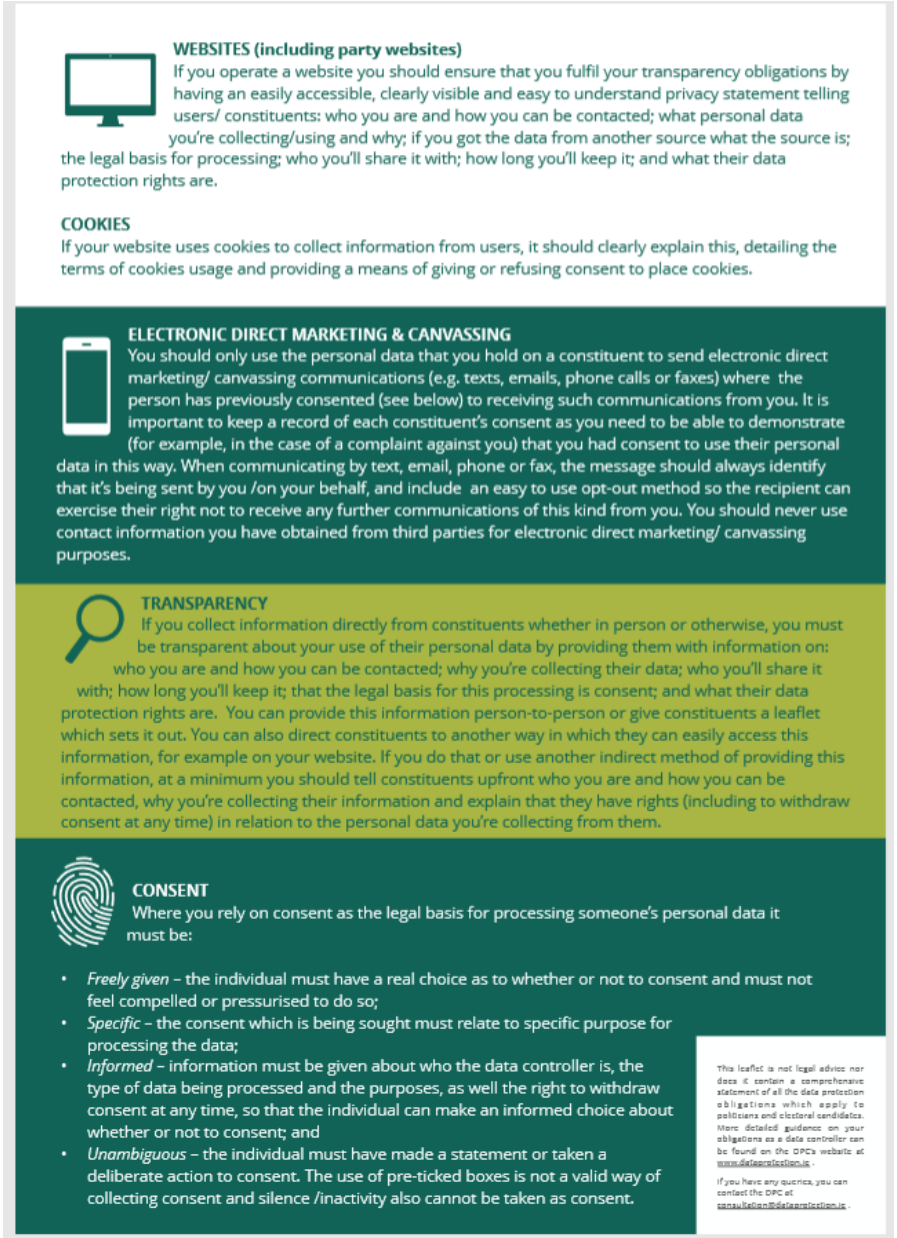
RESPECT THE INDIVIDUAL'S RIGHT TO DATA PROTECTION WHEN CANVASSING

POST

You may use the names and addresses of people on the Electoral Register for the purpose of sending postal election leaflets to them. You must be transparent about such use of constituents' personal data by providing them with information on: who you are and how you can be contacted; how you obtained their information and what it comprises; who you'll share it with; how long you'll keep it; what the legal basis is for processing the personal data (normally performance of a task in the public interest); and what their data protection rights are. This information can be provided by including it in, or with, your canvassing materials.

DOOR-TO-DOOR CALLS

When making door-to-door calls, ensure proper safeguards are in place to accurately record and protect any data collected, including any data revealing political opinions. If you ask constituents for their contact information (e.g. telephone number or email address) make sure they consent to follow-up contact if you plan it. You should also make it clear to constituents that they are not under any obligation to provide you with any information and that you are only collecting it where they consent. (see more information on transparency overleaf)



WEBSITES (including party websites)

If you operate a website you should ensure that you fulfil your transparency obligations by having an easily accessible, clearly visible and easy to understand privacy statement telling users/ constituents: who you are and how you can be contacted; what personal data you're collecting/using and why; if you got the data from another source what the source is; the legal basis for processing; who you'll share it with; how long you'll keep it; and what their data protection rights are.

COOKIES

If your website uses cookies to collect information from users, it should clearly explain this, detailing the terms of cookies usage and providing a means of giving or refusing consent to place cookies.

ELECTRONIC DIRECT MARKETING & CANVASSING

You should only use the personal data that you hold on a constituent to send electronic direct marketing/ canvassing communications (e.g. texts, emails, phone calls or faxes) where the person has previously consented (see below) to receiving such communications from you. It is important to keep a record of each constituent's consent as you need to be able to demonstrate (for example, in the case of a complaint against you) that you had consent to use their personal data in this way. When communicating by text, email, phone or fax, the message should always identify that it's being sent by you /on your behalf, and include an easy to use opt-out method so the recipient can exercise their right not to receive any further communications of this kind from you. You should never use contact information you have obtained from third parties for electronic direct marketing/ canvassing purposes.

TRANSPARENCY

If you collect information directly from constituents whether in person or otherwise, you must be transparent about your use of their personal data by providing them with information on: who you are and how you can be contacted; why you're collecting their data; who you'll share it with; how long you'll keep it; that the legal basis for this processing is consent; and what their data protection rights are. You can provide this information person-to-person or give constituents a leaflet which sets it out. You can also direct constituents to another way in which they can easily access this information, for example on your website. If you do that or use another indirect method of providing this information, at a minimum you should tell constituents upfront who you are and how you can be contacted, why you're collecting their information and explain that they have rights (including to withdraw consent at any time) in relation to the personal data you're collecting from them.

CONSENT

Where you rely on consent as the legal basis for processing someone's personal data it must be:

- *Freely given* – the individual must have a real choice as to whether or not to consent and must not feel compelled or pressurised to do so;
- *Specific* – the consent which is being sought must relate to specific purpose for processing the data;
- *Informed* – information must be given about who the data controller is, the type of data being processed and the purposes, as well the right to withdraw consent at any time, so that the individual can make an informed choice about whether or not to consent; and
- *Unambiguous* – the individual must have made a statement or taken a deliberate action to consent. The use of pre-ticked boxes is not a valid way of collecting consent and silence /inactivity also cannot be taken as consent.

This leaflet is not legal advice nor does it contain a comprehensive statement of all the data protection obligations which apply to politicians and electoral candidates. More detailed guidance on your obligations as a data controller can be found on the DPC's website at www.dataprotection.ie .

If you have any queries, you can contact the DPC at canvassing@dataprotection.ie .

https://www.dataprotection.ie/docimages/documents/Canvassing%20Elected%20Reps%20FINAL.pdf

Coimisiún Cosanta Sonraí
Data Protection Commission

Guidance on Data Protection rights is also available to Constituents

Coimisiún Cosanta Sonraí
Data Protection Commission

DATA PROTECTION PRINCIPLES

When your personal data is used for the purposes of political canvassing and electoral activities, your data protection **RIGHTS** include the following:

- To be given full and clear information about the collection and use of your personal data including the identity of the person for whom it is collected, why it is being collected, how it will be used, who it will be shared with, how long it will be kept and what your rights are in relation to that personal data;
- To access all your personal data held by any public representative, electoral candidate or political party/grouping unless a valid exemption exists;
- To have your personal data protected from being used for any purpose other than the valid and lawful purpose or purposes for which it was obtained;
- To have your personal data kept accurate and up-to-date and to have any inaccurate or incomplete data rectified or completed.
- To have your personal data kept safe and secure in an appropriate manner; and
- To lodge a complaint with the Data Protection Commission.

Elections & Canvassing: Data Protection and Electronic Marketing - the data protection rights of individuals

BALANCING RIGHTS

Data protection rights are not absolute and the General Data Protection Regulation (GDPR) recognises that they must be balanced against the public interest in ensuring the effective operation of a democratic society. This means that an individual's data protection rights may, in certain circumstances, be restricted in accordance with the law.

ELECTORAL ACTS

Electoral legislation permits the use of information (including name, address and polling station) which is contained on the electoral register for electoral purposes. This means that public representatives, political parties/ groupings and electoral candidates may use this information to communicate with voters, for example by issuing postal (direct marketing) election leaflets to individuals. The Data Protection Act 2018 modifies the usual right of individuals to object to direct marketing when the direct marketing occurs in the course of electoral activities, so that there is no legal right to object to electoral direct marketing by post.

Additionally, electoral legislation allows for any person to access, under certain conditions and within a certain timeframe, the marked version of the electoral register for a particular election which shows whether an individual has voted in that election.

ELECTRONIC MARKETING

Your rights in relation to electronic direct marketing/canvassing (i.e. texts, emails, phone calls or faxes) carried out by public representatives, electoral candidates or political parties/groupings continue to apply. You should only receive such communications if you have consented to receive them. You must also be informed of the identity of the sender in any such communications and be provided with a simple and easy-to-use way of opting-out of further such communications.

CANVASSING

Your personal data may be obtained from you through door-to-door canvassing if you agree to provide your personal data in this way but there is no obligation on you to do so. Public representatives, electoral candidates, their representatives and any political parties/ groupings collecting information about you must put appropriate safeguards in place to accurately record and protect any personal data collected from you, including your political opinions. They should provide you with clear information about what your data protection rights are, and how they will manage your data, including how and why it will be used, who it will be shared with and how long it will be retained.

PUBLIC REPRESENTATION

The Data Protection Act 2018 provides that your personal data may be processed by a public (elected) representative where you (or another person on your behalf) seek their assistance, for example in relation to access to services or to information about the provision of services. While this is an important democratic function, it is also important that public representatives protect the personal data of their constituents, particularly where processing involves special categories of personal data, by ensuring that they comply with the principles of data protection.

FOR MORE INFORMATION ON THE INDIVIDUAL'S RIGHT TO PROTECTION OF THEIR PERSONAL DATA, VISIT THE DATA PROTECTION COMMISSION'S WEBSITE AT **WWW.DATAPROTECTION.IE**

Coimisiún Cosanta Sonraí
Data Protection Commission

https://www.dataprotection.ie/docimages/documents/Canvassing%20-%20Individuals%20update%20final%20version.pdf

Section 40 of the Data Protection Act 2018 - Processing of personal data and special categories of personal data by elected representatives

Section 40

Processing of personal data and special categories of personal data by elected representatives

(1) For the purpose of enabling an elected representative to perform his or her functions as such a representative, the processing of personal data and special categories of personal data of a data subject by or on behalf of that representative shall be lawful where he or she receives a request or representation from the data subject or where, in accordance with *subsection (2)*, he or she receives a request or representation from another person on behalf of the data subject.

(2) A person may make a request or representation on behalf of a data subject where the data subject—

(a) has given his or her consent to the making of the request or representation, as the case may be, or

(b) is, by reason of his or her physical or mental incapacity or age, unable to make a request or representation on his or her own behalf.

(3) In processing special categories of personal data under *subsection (1)*, an elected representative shall impose limitations on access to that data to prevent unauthorised consultation, alteration, disclosure or erasure of that data.

Section 40

Processing of personal data and special categories of personal data by elected representatives (cont.d)

(4) For the purpose referred to in *subsection (1)* and to the extent that disclosure is necessary and proportionate to enable an elected representative to deal with a request or representation referred to in that subsection, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of the data subject, it shall be lawful for a person to disclose to the representative or a person acting on his or her behalf personal data and special categories of personal data of a data subject who makes the request or representation, or on whose behalf the request or representation is made, as the case may be, to enable that representative respond to that request or representation.

(5) In this section, "elected representative" means—

(a) a member of either House of the Oireachtas,

(b) a member of the European Parliament,

(c) a member of a local authority.

Coimisiún Cosanta Sonraí
Data Protection Commission

At present there is no guidance available to Elected Representa-ives on the DPC web-site in relation to Section 40

Councils proposed policy and procedures for processing of personal data with regard to their interactions with the AILG elected members

Proposed Council Data Protection Policy

1.0 Submissions by Elected Representatives to the Council

Elected Representatives are acting as Data Controllers when making representations on behalf of their constituents. When the Elected Representative submits a representation to the Council, relating to a constituent's personal data;

a) only representations received from Elected Representatives in writing (either by letter or email), will be processed by the Council.

b) the Council and its employees will process the representation received, based on the requirement that the Elected Representative has a legal basis for processing this data and the constituent has agreed to this transfer.

c) in respect of all representations received by email, the Council's staff will respond to all such representations using only the email address provided to the Elected Representative by the Council.

d) if Council staff consider that the relevant person is unaware of the submission on their behalf, then the Elected Representative must demonstrate that this person has consented to this data transfer.

Proposed Council Data Protection Policy (cont.d)

2.0 Responses to the Elected Representatives from the Council

When an Elected Representative makes a representation;

a) Representations not requiring the release of personal data:

If the representation is an enquiry about a service and no personal data (other than that originally contained in the request) needs to be used in the reply, the reply will issue directly to the Elected Representative. This therefore means that where personal data is not to be issued in the reply, that the request and reply may be made in any form (i.e. written, verbal, etc.).

Example 1

Notes

There is no personal data being released over the information included in the representation submitted, so there is no requirement for any Verification form to be included with this representation. Basically no change on representations submitted in the past.

Representation

Dear Local Authority,

Can you arrange for the pothole outside of Jim Smith's House, 43 Brookfield Heights to be repaired

Yours sincerely

Cllr. -----

Response

Dear Cllr. ----,

I wish to acknowledge receipt of your representation and I would like to inform you that the pothole outside of Mr. Smith's house at 43 Brookfield Heights has been added to the worklist for the local road repair crew and this work will be carried out shortly.

Yours sincerely

Local Authority

Example 2

Notes

There is no personal data being released over the information included in the representation submitted, so there is no requirement for any Verification form to be included with this representation. Basically no change on representations submitted in the past.

Representation

Dear Local Authority,

I am making representation on behalf of Jim Smith, 43 Brookfield Heights who would like to report illegal dumping in a laneway in Brookfield Way and request that this be cleaned up.

Yours sincerely

Cllr. -----

Response

Dear Cllr. ----,

I wish to acknowledge receipt of your representation and I would like to inform you that the illegal dumping in Brookfield Way has been reported to the Litter Enforcement Section and a member of this team will investigate this issue and arrange for the area to be cleaned up.

Yours sincerely

Local Authority

Proposed Council Policy (cont.d)

2.0 Responses to the Elected Representatives from the Council

b) Representations requiring the release of personal data:

If the representation is an enquiry that requests personal data to be released (other than the personal data originally contained in the request) and if the Elected Representative submits the completed ***'Verification Form'***, the Council staff will respond directly to the Elected Representative. All responses are to be sent by email to the email address provided to the Elected Representative by the Council (i.e. xxxxx@countycouncil.ie).

A ***'Verification Form***' can be submitted for individual requests or a '***Verification form'*** can be submitted for multiple requests relating to the same process and the same data subject.

If the representation is an enquiry that requests personal data to be released (where the request relates to data that is extra to what was in the representation received) and the representation does not include the '***Verification Form'***, the reply will issue to the Data Subject or the person legitimately acting on behalf of the Data Subject. The content of the response will refer to the representation being made by the Elected Representative who made the request. An email notification will also be sent to the Elected Representative to state that a response has issued in relation to the representation.

Each Council is to nominate staff in each department at an appropriate level to review each response which contains personal data to be released (other than the personal data originally contained in the request).

Verification Form

Form for an Elected Representative to Receive Personal Data

The following describes the enquiry that the Elected Representative will make on my behalf and I acknowledge that the Elected Representative may receive personal data, in accordance with the provisions of Section 40 of the Data Protection Act 2018, for the purpose of a response to this enquiry:

Details of my enquiry:

_____

_____

_____

_____

_____

Signature (of person making request): _____ *(not the Elected Representative)*

Date: _____

For verification purposes

Name of Person subject of the request (data subject): _____

Address of Person subject of the request (data subject): _____

_____

If the person making the request is not the subject

(Please provide consent of the data subject or statement as to why consent cannot be provided)

Please print name of person making the request: _____

State relationship to the data subject: _____

ELECTED REPRESENTATIVE DECLARATION

When I receive personal data from ----- County/City Council, I confirm that I will take suitable and specific measures to safeguard the fundamental rights and freedoms of the person this representation relates to and process the information in accordance with Section 40 of the Data Protection Act 2018.

Name: Cllr./Deputy/Senator_____

Signature: _____

Verification Form

Form for an Elected Representative to Receive Personal Data

The following describes the enquiry that the Elected Representative will make on my behalf and I acknowledge that the Elected Representative may receive personal data, where necessary and proportionate, for the purpose of a response to this enquiry:

Details of my enquiry:

Is my social housing application being considered at the moment and will I get a house shortly.

Signature (of person making request): Jim Smith *(not the Elected Representative)*

Date: 12/11/18

For verification purposes

Name of Person subject of the request (data subject): Jim Smith

Address of Person subject of the request (data subject): 43 Brookfield Heights

If the person making the request is not the subject

(Please provide consent of the data subject or statement as to why consent cannot be provided)

Please print name of person making the request:

State relationship to the data subject:

ELECTED REPRESENTATIVE DECLARATION

When I receive personal data from ----- County/City Council, I confirm that I will take suitable and specific measures to safeguard the fundamental rights and freedoms of the person this representation relates to and process the information in accordance with Section 40 of the Data Protection Act 2018.

Name: Cllr./~~Deputy~~/~~Senator~~ Morgan

Signature: Tim Morgan

Example 3a

Notes

A valid Verification Form has been provided with the representation so the requested information is provided to the Elected Representative.

Representation

Dear Local Authority,

I am making representation on behalf of Jim Smith, 43 Brookfield Heights who has asked me to query his social housing application. Is he being considered at present for any pending allocations and will he be in line for an allocation shortly

Can you forward me the relevant information?

Yours sincerely

Cllr. -----

Response (if Verification form is submitted with the representation)

Dear Cllr. ----,

I wish to acknowledge receipt of your representation and I attach the requested information.

Yours sincerely

Local Authority

Example 3b

Notes

No Verification Form has been provided so the requested information will be issued to the Data Subject (or the person legitimately acting on behalf of the Data Subject). The content of the response will refer to the representation being made by the Elected Representative who made the request. An email notification will also be sent to the Elected Representative.

Representation

Dear Local Authority,

I am making representation on behalf of Jim Smith, 43 Brookfield Heights who has asked me to query his social housing application. Is he being considered at present for any pending allocations and will he be in line for an allocation shortly

Can you forward me the relevant information?

Yours sincerely

Cllr. -----

Response (if **NO** Verification form is submitted with the representation)

Dear Cllr. ----,

I wish to acknowledge receipt of your representation and I have forwarded the requested information directly to Mr. Smith. I have also notified Mr. Smith that this information was received following a representation received from you.

Can you please make arrangements directly with Mr. Smith if you wish, to discuss his request, as per your representation?

Yours sincerely

Local Authority

Course Objectives

Today we provided:

- an overview on the General Data Protection Regulation (GDPR);
- specific focused training on Section 39 of the DPA 2018 - Communication with data subjects by political parties, candidates for and holders of certain elective political offices
- specific focused training on Section 40 of the DPA 2018 - Processing of personal data and special categories of personal data by elected representatives; and,
- specific focused training on the Irish County Councils proposed policy and procedures for processing of personal data with regard to their interactions with the AILG elected members.

Questions?

Thank you