

DATA PROTECTION – WHAT ELECTED MEMBERS NEED TO KNOW



AILG Elected Members Training – November 2022

Gerry Egan Consulting

Governance | Data Protection | Strategy & Change

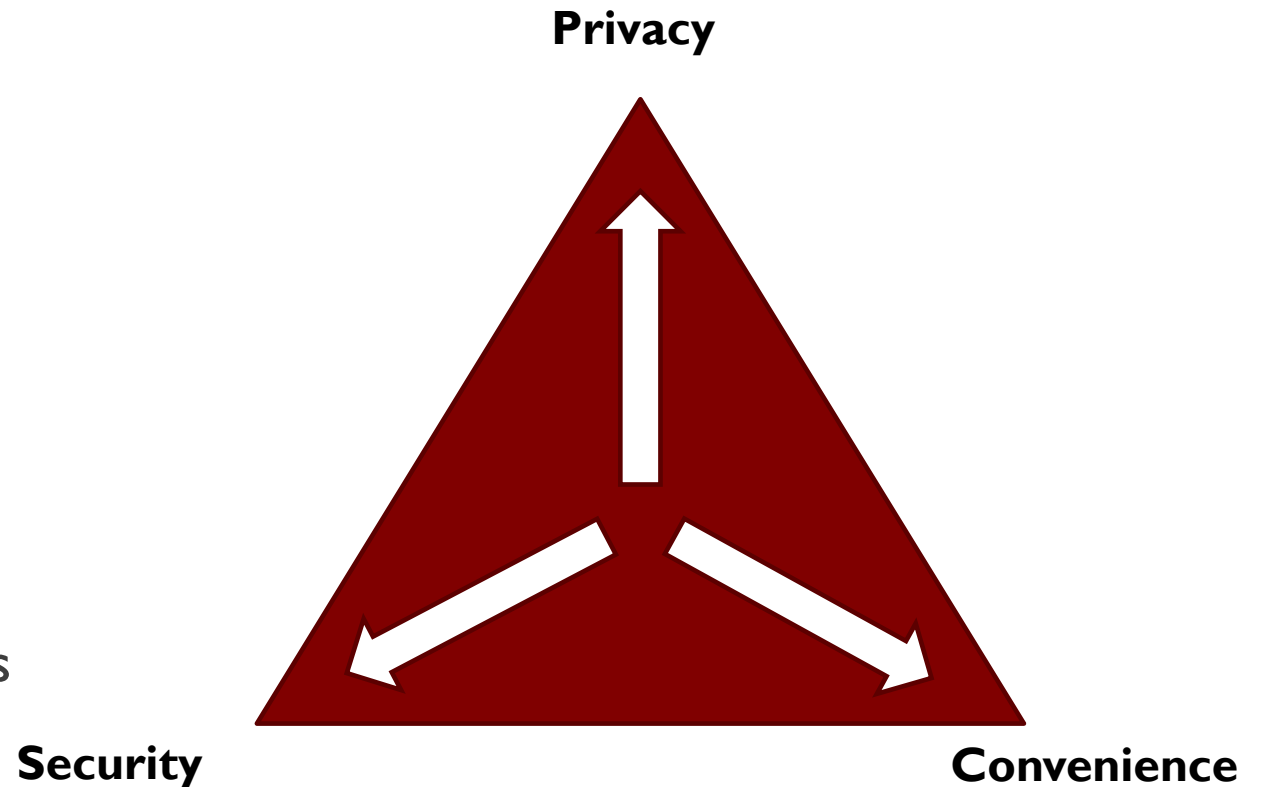
ABOUT ME..

- Independent consultant: advice, implementation, training
- Chartered Director
- Company Secretary
- Member of two charity boards
- Private, public, NFP sector clients
- Formerly of Coillte



PERSONAL DATA AND PRIVACY

- A more connected world, creates great opportunities... medicine, news, travel, services
- Data is the new
- Dominance of big tech
- If you're not paying for the product
- Challenges to democracy and civil liberties
- The end of privacy?



IN TODAY'S TRAINING...

Overview of GDPR

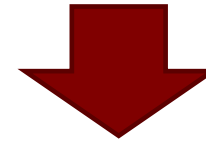
What is it and why does it matter?

Seven Principles of Data Management

Your Role as a Data Controller

Data Subject Rights

For Elected Members



Office Management

Campaigning

Making Representations

Because of GDPR I can no longer call out your names. Will the gentleman with piles come in please?



GDPR - REMINDER

- An EU Regulation (2016/679) adopted on 27 April 2016 on
 - **The protection of natural persons with regard to the processing of personal data and on the free movement of such data....**
- Designed to protect European citizens and residents by safeguarding personal data that we provide to public authorities, companies, charities etc.
- Applies to all organisations public, private, non-profit
- CAME INTO FORCE IN EU AND EEA ON 25 MAY 2018
- Complemented by Data Protection Act 2018. **This Act makes specific reference to public representatives, election literature and representations.**
- Significant penalties for non-compliance including up to €20m or 4% of global turnover

QUICK HISTORICAL BACKGROUND AND CONTEXT

- The right to privacy is a fundamental human right recognised in the European Convention on Human Rights (1950)
- Article 8 says:
 1. ‘Everyone has the right to respect for his private and family life, his home and his correspondence’
 2. ‘there shall be no interference by a public authority.....national security, public safety, economic wellbeing of country etc.’
- Major shift in how we think about data and the value of it with the emergence of technology
- Interesting that purpose of early data protection and privacy conventions was to protect citizens privacy from the State whereas now a whole different set of issues has arisen from data being controlled by private interests
- First Data Protection Act in Ireland in 1988 so not new, however GDPR seriously ‘ups the stakes’

UNIQUE POSITION OF ELECTED REPRESENTATIVES

- Role of elected representatives is recognised by the Data Protection Commission as playing an extremely important function in a free and democratic society
- Specific provisions in Data Protection Act 2018:
 - Section 39 deals with **communication with data subjects** by political parties, candidates for and holders of certain elective political offices
 - Section 40 deals with **representations** by elected representatives

DPC & LGMA REFERENCE DOCUMENTS

We'll return to this later

Elected Representatives, the General Data Protection Regulation and the Data Protection Act 2018 (the DPA 2018)

Constituency Office - Best Practice in the Workplace

Guidelines on the processing¹ of personal data² by Elected Representatives³ under Section 40 of the Data Protection Act 2018 (the DPA 2018)

Guidance for Compliance with Section 40 Data Protection Act, 2018 – Elected Members' Representations –
1st November 2019 - inc Working Group discussions on 11/10/2019[¶]

- ¶
- 1.0 Context ¶
- 1.1 The General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018. The purpose of this regulation is to oversee and control the use of personal data¹ by organisations and individuals such as Elected Representatives, who are described as data controllers, and so protect the privacy of individual citizens, known as data subjects. ¶
- 1.2 In Ireland, the GDPR is given further effect by the Data Protection Act 2018. Section 40 of this Act makes provision for the processing of personal data by Elected Representatives and related guidance from the Data Protection Commission recognises that making representations is a normal and important democratic function which typically occurs in relation to access to services or to information about the provision of services. ¶
- 1.3 Many representations received by the Council from Elected Representatives do not require the disclosure of personal information about constituent to the Elected Representative and can be adequately responded to by applying existing procedures agreed with Elected Representatives without any GDPR issue arising. However, there is a proportion of representations where the disclosure of personal data by the Council is required in response to a representation. ¶
- 1.4 The following guidance on the processing of personal data in the context of making representations is intended to: ¶
- support the representational role of the Elected Representative and enhance services to his/her constituents. ¶
 - protect constituents' (data subjects) rights in the management of their personal data ¶ in representations. ¶

¶

¶ Personal data is defined in the GDPR as any information relating to an individual 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 ID number, location data, an on-line identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person. ¶

¶



IMPORTANT TERMS AND KEY PLAYERS



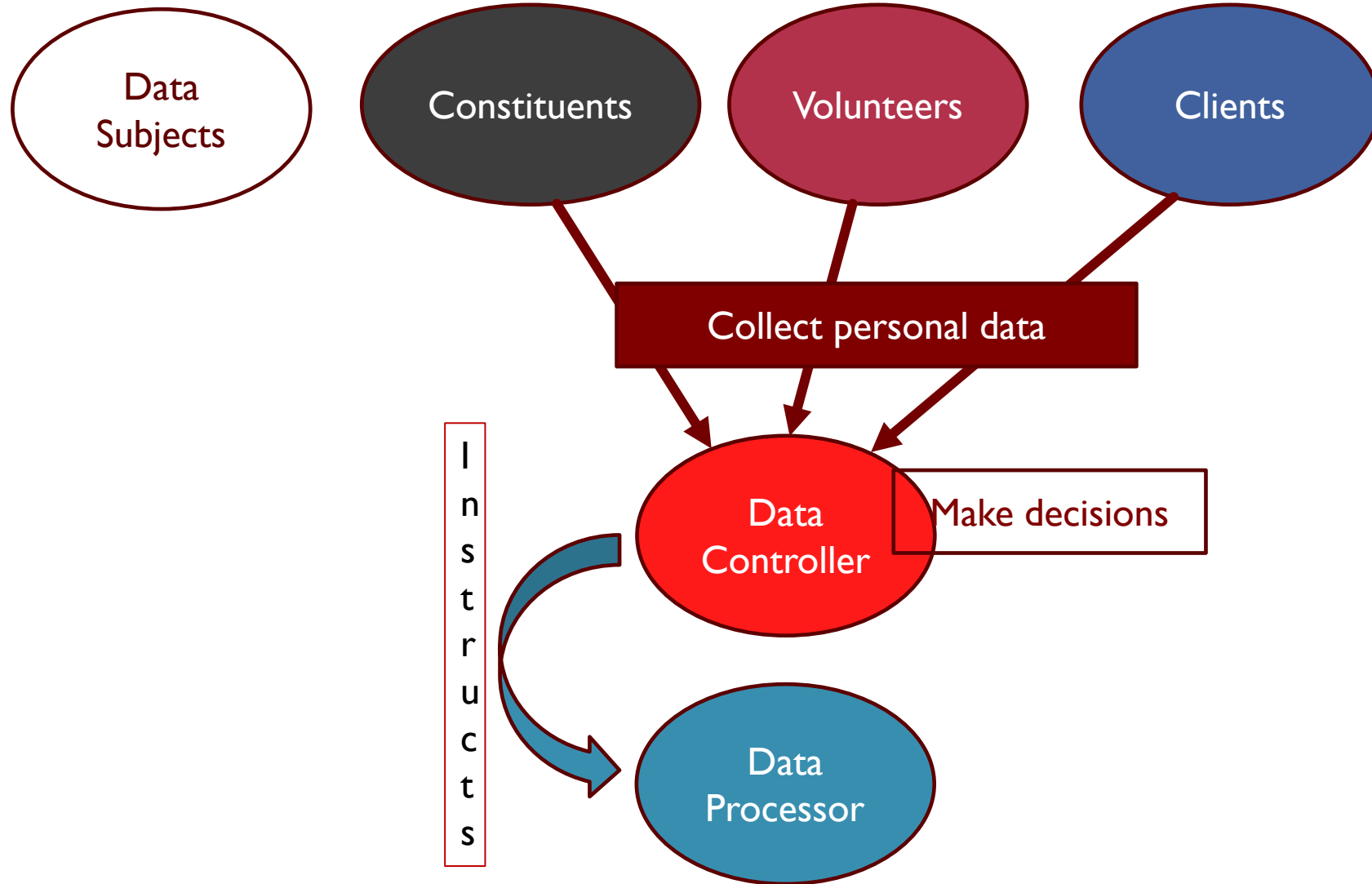
IMPORTANT TERMS

- **Personal Data:** any information relating to an identified or identifiable natural person (the data subject)
- **Special Categories of Personal Data:** data on racial or ethnic origin, political views, religious or philosophical beliefs, physical or mental health, sexual orientation, sex life, trade union association, genetic data, biometric data
- **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data – either manually or automated

Consider:

What personal data including special categories of personal data are you likely to process in your capacity as an elected representative?

Why are you processing this data? How did you get it? Where and for how long will you keep it? How will you secure it? How will you delete it when finished?



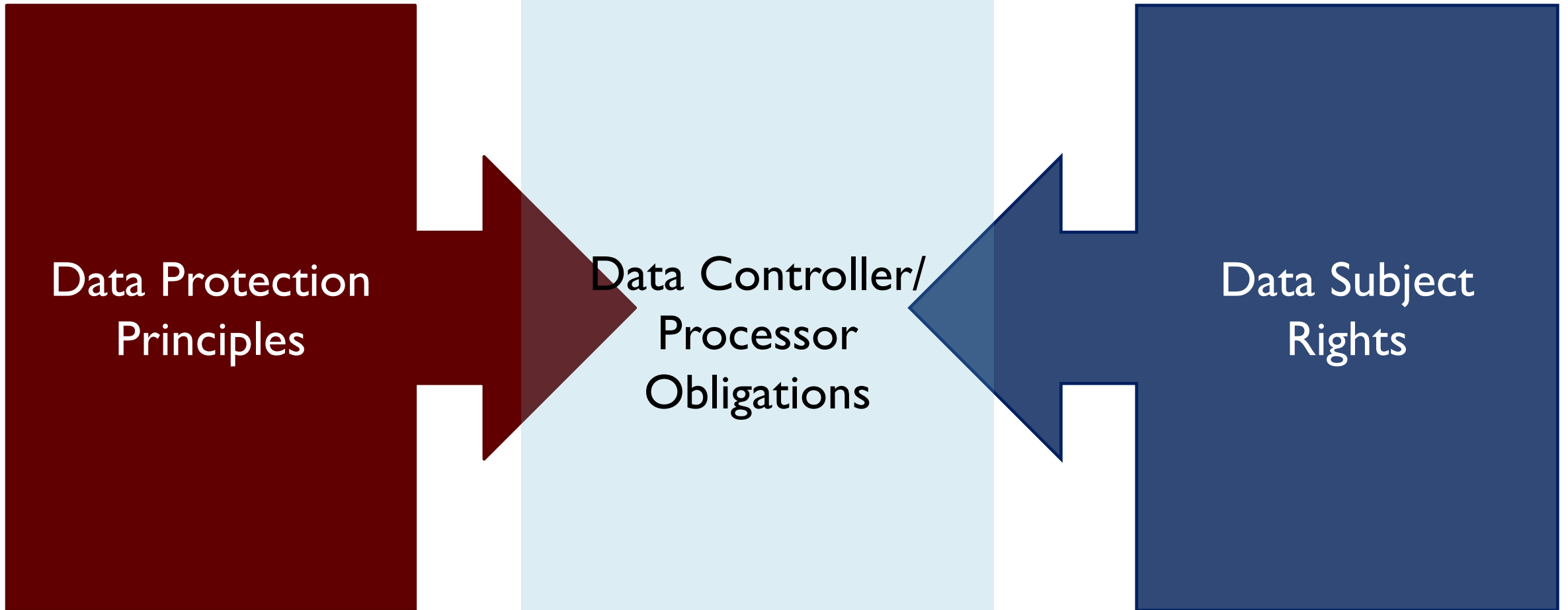
Consider: what categories of data subject are you likely to process personal data about in your capacity as an elected representative?

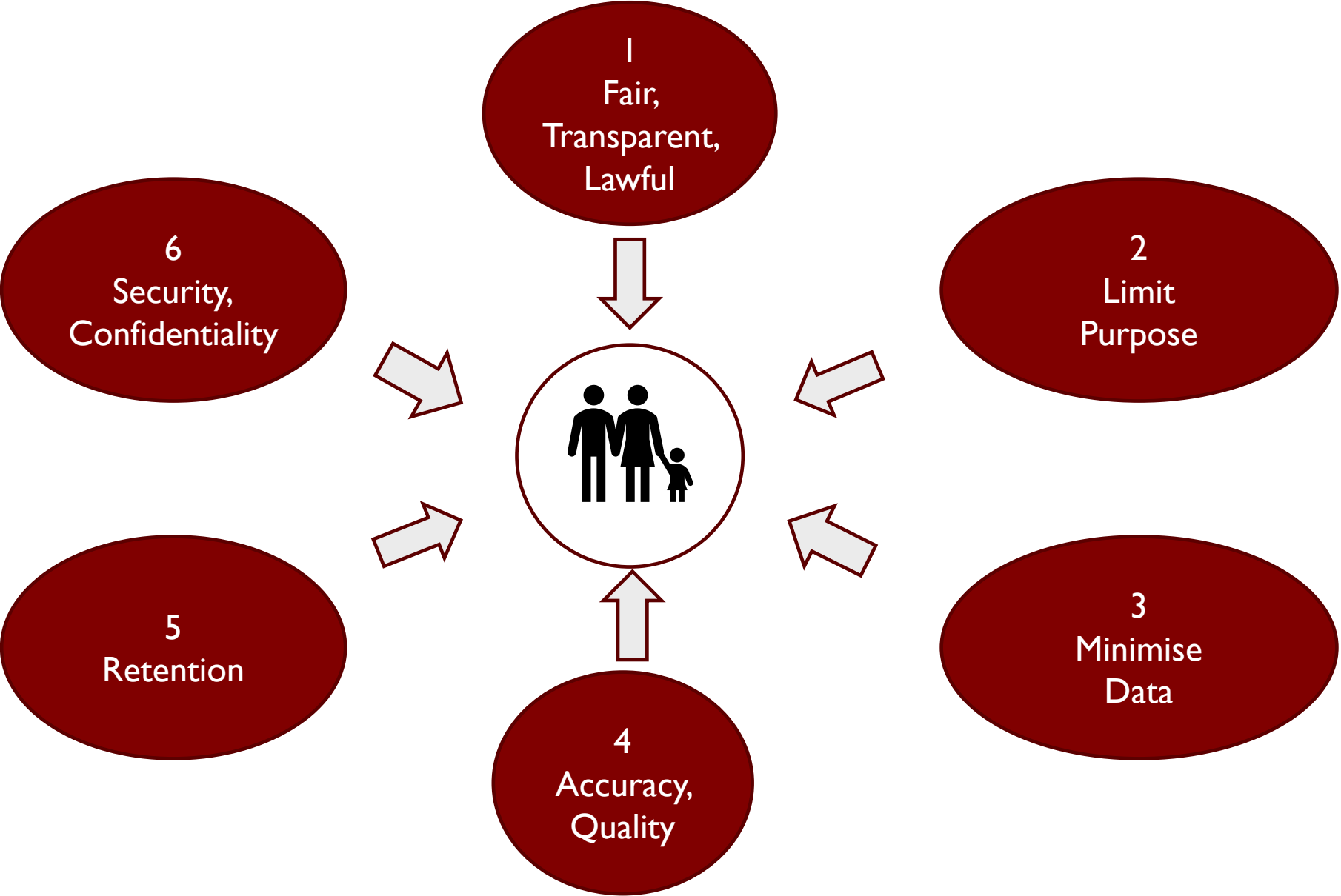
GDPR IN ESSENCE

Data Protection
Principles

Data Controller/
Processor
Obligations

Data Subject
Rights





SEVEN PRINCIPLES SUMMARISED

1 Fair and Transparent processing	Tell the data subject what you're doing Use the data only for lawful purposes Fulfil a lawful processing condition (ordinary and special categories)
2 Purpose Limitation	Use the data for the purpose for which it was collected and not for any other purpose NB canvassing and representations.
3 Minimisation	Process as little data as necessary – avoid excessive data collection
4 Accuracy and Quality	Keep the data accurate and up to date
5 Retention	Keep the data only for as long as you need it and delete it when no longer required
6 Security and Confidentiality	Keep the data safe and maintain confidentiality
7 Liability/ Accountability	Understand and carry out your obligations as a data controller, processor. Be able to demonstrate compliance.

CHALLENGE THE USE OF THE DATA

GDPR IN ESSENCE

Data Protection
Principles



Data Controller/
Processor
Obligations

GOVERNANCE - DATA CONTROLLER PRIORITIES

1. Understand your data and what it will be used for
2. Maintain Register of Processing Activity
Personal Data: Who, what, where, why, when and how
3. Prepare privacy notice(s)
4. Keep the data secure
5. Record and notify data breaches
6. Understand Data Subject Rights and have a process to handle requests

I. UNDERSTAND DATA AND WHAT IT WILL BE USED FOR

- What personal data do I have? (Canvassing lists, volunteer lists, client files etc.)
- What am I using it for?
- How did I obtain it?
- How do I keep it up to date?
- How long will I keep it?
- How secure is it? (encryption and accessibility)
- Who might I share it with and why?

3. PREPARE PRIVACY NOTICE

- Purpose: **PROVIDE ASSURANCE**
- You must tell the person (data subject) :
 - Who is collecting and processing their data
 - Why it is being processed
 - Who the data might be given to
 - That they have a right to access one's own personal data
 - Who to contact in the data controller
 - Any other relevant information which will make the data processing fair
- Website, representation forms, canvasser instructions – whatever is the most effective way to reach your audience
- **DPC recommends specific notice in relation to representations**

4. KEEP THE DATA SECURE AND CONFIDENTIAL

- You must have appropriate security measures to protect the data under your control
- The greater the risk to the data and the impact on the data subject the higher the standard required

Physical security: lock and key

IT security: strong passwords, encrypted laptops, no USBs, restricted access

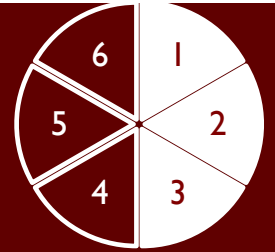
Policies and Procedures – delegating to staff, disposal, use of email

5. RECORD AND NOTIFY DATA BREACHES

- The Controller is obliged to disclose any incident where the data is exposed to risk, even where the data may not have been disclosed outside the organisation or to an unauthorised individual
- Information should be provided on the following aspects of the incident:
 - A description of nature of the personal data breach;
 - The categories and approximate number of Data Subjects concerned;
 - The categories and approximate number of data records concerned;
 - The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
 - A description of the likely consequences of the personal data breach;
 - A description of the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

You must notify the DPC within 72 hours of discovering the breach. Staff need to know this and the culture must support timely reporting of data losses or other breaches.

IF A BREACH OCCURS...



Assess the risk to the data subject

No Risk

Record in internal breach register

Review incident for lessons learned and apply fix

Risk

Record in internal breach register

Review incident for lessons learned and apply fix

Report to DPC within 72 hours of becoming aware

High Risk

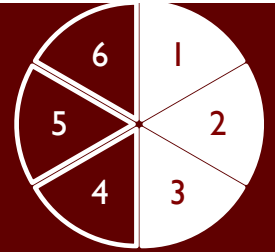
Record in internal breach register

Review incident for lessons learned and apply fix

Report to DPC within 72 hours of becoming aware

Advise data subject(s)

REPORTING A BREACH TO DPC



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Gaeilge ▾

Search

SEARCH

[About](#)

[Contact](#)

[For Individuals](#)

[For Organisations](#)

[Guidance](#)

[Law](#)

[News & Media](#)

[Pre-GDPR](#)



Take Action

REPORT A BREACH

RAISE A CONCERN


REGISTER YOUR DPO

The Data Protection Commission

Latest News

6. RESPECT DATA SUBJECT RIGHTS

- Understand Data Subject Rights and have process to handle requests



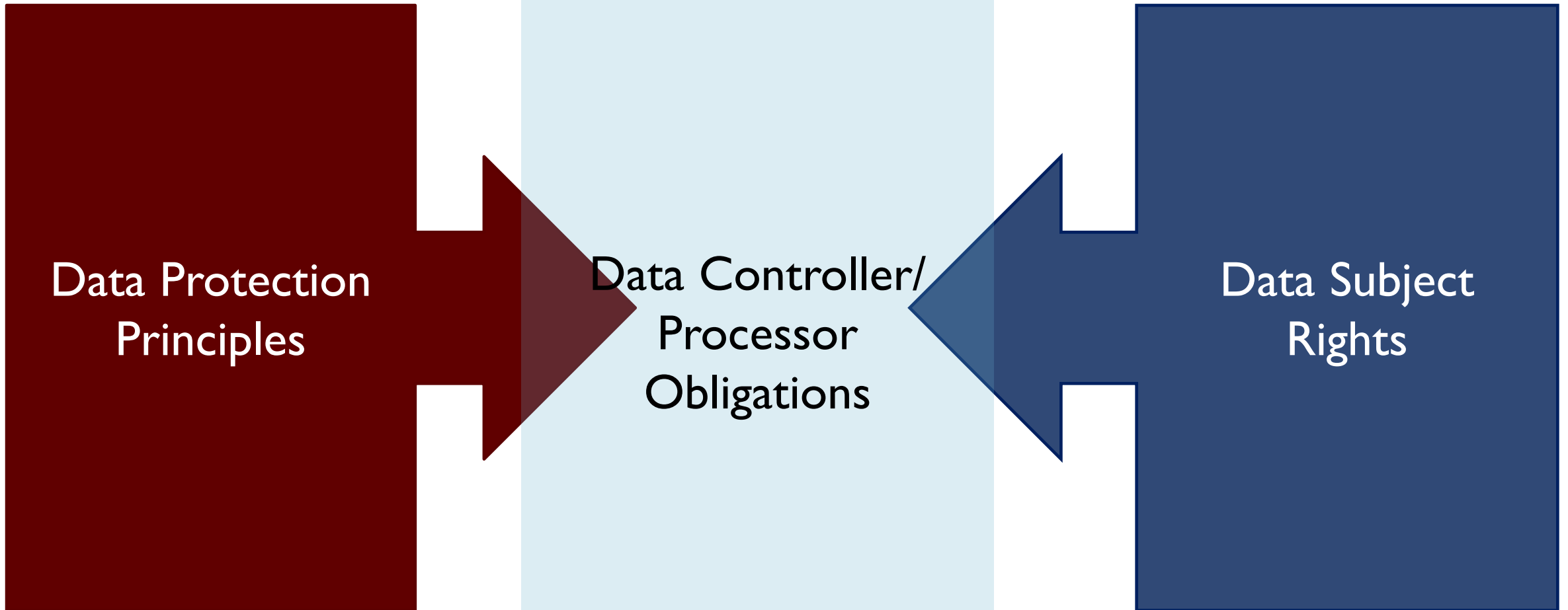
We'll come back to this later!

GDPR IN ESSENCE

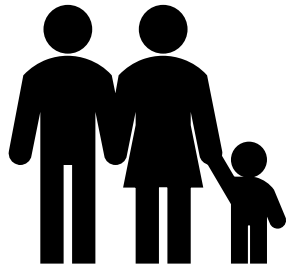
Data Protection
Principles

Data Controller/
Processor
Obligations

Data Subject
Rights



THE RIGHTS OF DATA SUBJECTS



The Right of Erasure (The Right to be Forgotten)

The Right to Restriction of Processing

The Right to Rectification

The Right to Object

The Right to Data Portability

The Right of Access



Additional rights in relation to profiling and automated decision making

1 month!

A 1 month response time applies to all Data Subject Rights so it is essential that:

1. All staff in receipt of data subject access requests understand these rights and the obligation to respond within 30 days and
2. You have efficient retrieval processes in place i.e. you know where the data is and who is responsible for it.



IMPORTANCE OF COMPLIANCE



COMPLIANCE ENFORCEMENT ACTIVITY (DPC REPORT 2020)

Cases: 10,151  9% (4,476 concluded)

Data Breaches: 6628  9%

Statutory Enquiries: 83 (56 domestic + 27 cross border)  19%

X Border Complaints: 354  23%

DPOs: +570 total now 2,166

IRISH CASES AND FINES

Tusla - €75,000

- Investigation into three cases where information about children was wrongly disclosed to unauthorised parties
 - contact and location data of a mother and child victim was disclosed to an alleged abuser
 - data about children in foster care was improperly disclosed to blood relatives (x 2 cases)

Tusla – €40,000

- Unauthorised disclosure of personal data

HSE - €65,000

- Security breach - inappropriate disposal of patient files

UCD – €70,000

- Personal data breaches - email system

Ryanair – reprimand

- Failure to retain recording of phone call to satisfy subject access request

LOOKING FURTHER AFIELD....

32 countries have issued fines to date



€746m

Online retailer – non-compliance with general DP principles

€225

Messaging app – insufficient fulfilment of information obligations

€50m

Search engine – insufficient legal basis

€28m

Telecoms company – direct marketing - insufficient basis for processing

€15m

Berlin housing association – non-compliance with general DP principles

€2.7m

National Revenue Agency – inadequate security

LOOKING FURTHER AFIELD (2)...



€400,000 Hospital failure to limit access, inadequate security



€200,000 Failure to provide transparency notices, aggregation of publicly available data



€160,000 Taxi company – retention of data for longer than necessary



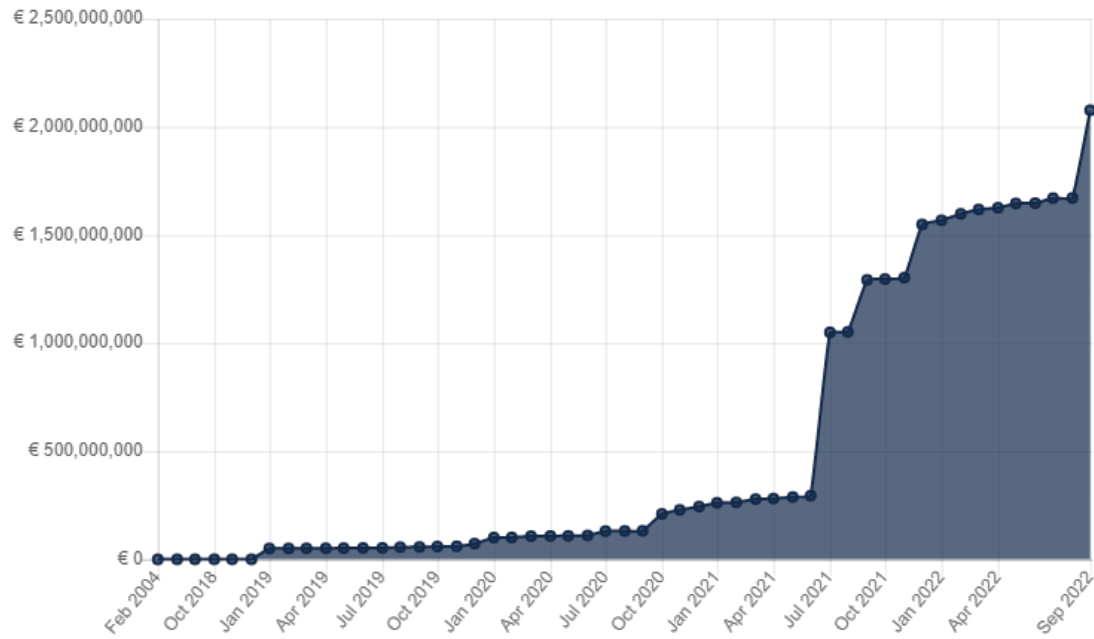
€35,000 Political party database accessible on hacker forum – poor security



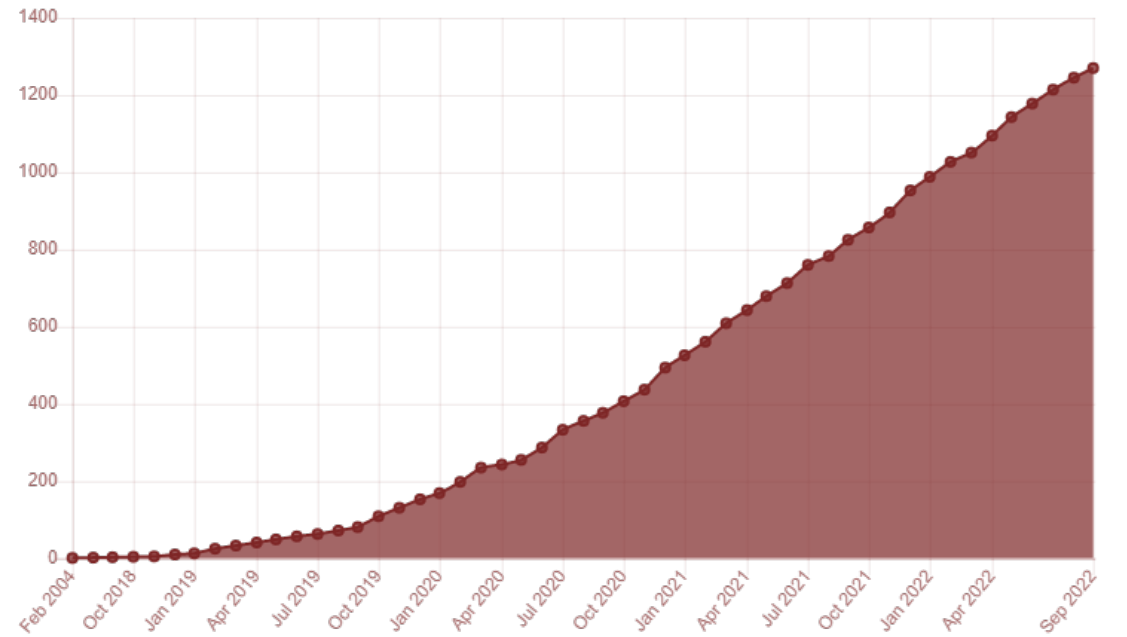
€20,000 Hackers stole 330,000 email addresses – kept in plain text



€4,800 Use of CCTV deemed excessive, no notices in place



Cumulative fines (value)



Cumulative fines (number)

<https://www.enforcementtracker.com/>

IN TODAY'S TRAINING...

Overview of GDPR

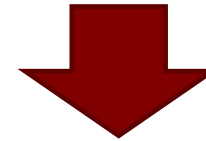
What is it and why does it matter?

Seven Principles of Data Management

Your Role as a Data Controller

Data Subject Rights

For Elected Members



Office Management

Campaigning

Making Representations

DPC GUIDANCE FOR ELECTED MEMBERS

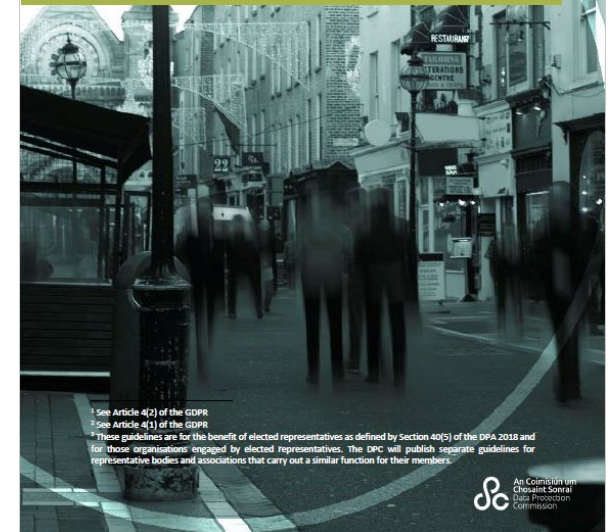
Elected Representatives, the General Data Protection Regulation and the Data Protection Act 2018 (the DPA 2018)



Constituency Office - Best Practice in the Workplace



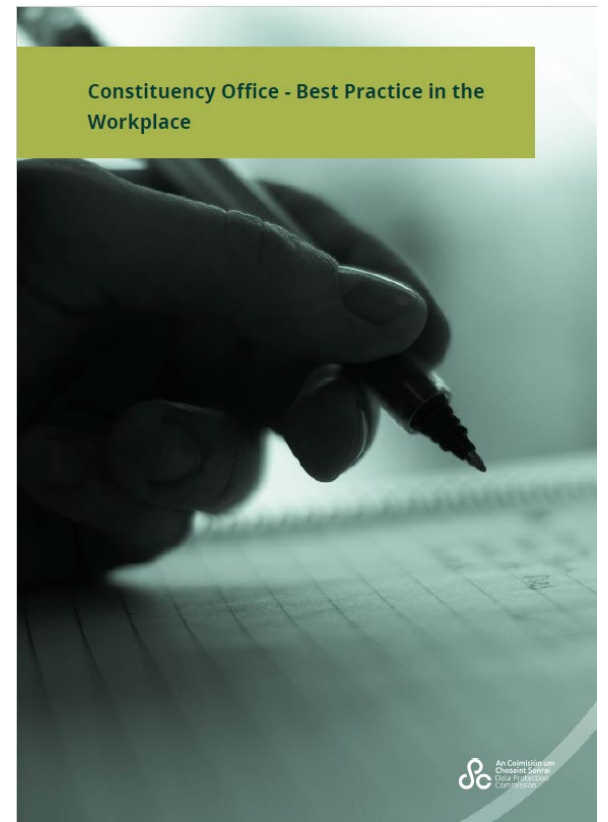
Guidelines on the processing¹ of personal data² by Elected Representatives³ under Section 40 of the Data Protection Act 2018 (the DPA 2018)



¹ See Article 4(2) of the GDPR
² See Article 4(1) of the GDPR
³ These guidelines are for the benefit of elected representatives as defined by Section 40(5) of the DPA 2018 and for those organisations engaged by elected representatives. The DPC will publish separate guidelines for representative bodies and associations that carry out a similar function for their members.

OFFICE MANAGEMENT BEST PRACTICE

- What personal data do I have? (Canvassing lists, volunteer lists, client files etc.)
- What am I using it for?
- How did I obtain it?
- How do I keep it up to date?
- How long will I keep it?
- How secure is it? (encryption and accessibility)
- Who might I share it with and why?



DPC RECOMMENDATIONS

- Have a privacy notice (and a specific notice for representations)
- Don't assume that someone who makes a request for a representation automatically wishes to have their data used for canvassing (purpose limitation principle)
- Focus on keeping personal data accurate and up to date
- Process data only for as long as it is needed for the purpose of the request
- Keep the data secure incl. limiting access to only those who need it

POLITICAL CAMPAIGNING - S. 39 DATA PROTECTION ACT 2018

- (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.

You don't need consent to compile a list of constituents and write to them for electoral purposes.

DPC GUIDANCE FOR ELECTED MEMBERS

Elected Representatives, the General Data Protection Regulation and the Data Protection Act 2018 (the DPA 2018)

Constituency Office - Best Practice in the Workplace

Guidelines on the processing¹ of personal data² by Elected Representatives³ under Section 40 of the Data Protection Act 2018 (the DPA 2018)

Guidance for Compliance with Section 40 Data Protection Act, 2018 – Elected Members’ Representations –
1st November 2019 inc Working Group discussions on 11/10/2019[¶]

1.0 Context ¶

1.1 The General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018. The purpose of this regulation is to oversee and control the use of personal data¹ by organisations and individuals such as Elected Representatives, who are described as data controllers, and so protect the privacy of individual citizens, known as data subjects. ¶

1.2 In Ireland, the GDPR is given further effect by the Data Protection Act 2018. Section 40 of this Act makes provision for the processing of personal data by Elected Representatives and related guidance from the Data Protection Commission recognises that making representations is a normal and important democratic function which typically occurs in relation to access to services or to information about the provision of services. ¶

1.3 Many representations received by the Council from Elected Representatives do not require the disclosure of personal information about constituent to the Elected Representative and can be adequately responded to by applying existing procedures agreed with Elected Representatives without any GDPR issue arising. However, there is a proportion of representations where the disclosure of personal data by the Council is required in response to a representation. ¶

1.4 The following guidance on the processing of personal data in the context of making representations is intended to: ¶

- support the representational role of the Elected Representative and enhance services to his/her constituents. ¶
- protect constituents’ (data subjects) rights in the management of their personal data in representations. ¶

¶ **Personal data** is defined in the GDPR as any information relating to an individual 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 ID number, location data, an on-line identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person. ¶

MAKING REPRESENTATIONS – S. 40 DPA 2018

40. (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.

(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**

IN SUMMARY

- A request for a representation provides the lawful basis for processing personal data
- Representations can be made on behalf of someone else e.g. an elderly parent
- Special care has to be taken to protect special category e.g. health data
- Local authority staff can release information in response to a representation

Principal concern of LA's seems to be not to disclose information against wishes of data subject.

LGMA GUIDANCE (AILG CONSULTED)

Guidance on the processing of personal data in the context of making representations is intended to:

- support the representational role of the Elected Representative and enhance services to his/her constituents.
- protect constituents' (data subjects) rights in the management of their personal data in representations;
- assist Elected Representatives and Council officials in discharging their responsibilities under the Data Protection Act 2018 (the Act) and the GDPR when managing representations made on behalf of constituents.

KEY PRINCIPLES

- the Elected Representative has a legal basis for processing personal and special category data where the representative has been asked to make representations by the constituent or a third party on his/her behalf.
- an Elected Representative will need to be satisfied that they are, at all times, acting upon a request from the constituent/data subject. In many instances, the permission of the individual can be **implied from a relevant action or request**. For example, the raising of the matter by an individual will create an expectation that his/her personal data will be further processed by the Elected Representative and by the Council.
- where the Council determines that it will be necessary to disclose personal data or special category data over and above what has already been supplied by the constituent via the Elected Representative in the reply, the Elected Representative must make the request **in writing** using the required representational form.
- if the Council is of the firm opinion that the constituent is unaware of the submission/ representation being made on his/her behalf, the Elected Representative will be asked to demonstrate that the constituent has consented to this data disclosure before personal data is provided to the Elected Representative.

Representations

Ordinary Personal Data

On own behalf
3.1
Form 1

On behalf of 3rd party
3.2
Form 1 + Get consent

Special Category Data

On own behalf
3.3
Form 2

On behalf of 3rd party
3.4
Form 2 + Get consent

PROCESS FOR RECEIVING AND RESPONDING TO REPRESENTATIONS

3.1 Representations requiring the disclosure of personal data (non-sensitive data) in reply

- Representations involving the disclosure of personal (non-sensitive) data must be made in writing. There are three means by which such a representation may be made:
- (i) The Elected Representative may complete, sign and submit the details of the representation from the constituent using the Representation Form (Personal Data) detailed in Appendix I, **or**
- (ii) The Elected Representative may sign the Representation Form (Personal Data) detailed in Appendix I, attach a written representation received from the subject and submit both to the Council **or**
- (iii) The Elected Representative may make a representation by attaching the appropriate Representation Form detailed in Appendix I to an email or submitting the form via a contact management system according to the agreed local procedure.
- NB: The Elected Representative does not need the signature of the constituent/data subject in order to submit the representation.

3.2 Requests for representations by a Third Party (on the constituent's behalf) requiring the disclosure of personal data (non-sensitive data) in reply

- Where a request for a representation is by a third party on behalf of the constituent (for example on behalf of an elderly person by a family member), either the email/letter or the Representation Form must be accompanied by **either the written consent of the constituent/data subject or, where this is not possible, a written explanation (with supporting documentation³) why consent cannot be given** and how the representation is in the interests of the constituent.

3.3 Representations requiring the disclosure of special category/sensitive personal data

-additional controls be applied in case of processing of special or sensitive category special data⁴. It is *generally envisaged that provision of special category or sensitive personal data should not be required for the purposes of responding to a representation*. However, where it is absolutely necessary the data should be the minimum required to and the process should be as follows:
- The Representation Form detailed in Appendix 2 should be signed by the Elected Representative **and** by the constituent, giving consent for release of said data to the Elected Representative. Given the nature of such data, use of the Representation Form is the only means by which the Council can provide data to the elected representative. As outlined in 3.1 above the Elected Representative may make a representation by attaching the Representation Form detailed in Appendix 2 to an email or submitting the form via a contact management system according to the agreed local procedure.



3.4 Requests for representations by a Third Party (on the constituent's behalf) requiring the release of special or sensitive data in reply

- Where a request for a representation is by a third party on behalf of the constituent (for example on behalf of an elderly person by a family member), the email/letter or the Representation Form must be accompanied by either the written consent of the constituent **or** where this is not possible, a written explanation (with supporting documentation) why consent cannot be given and how the representation is in the interests of the subject;⁴

Appendix 1 – Representation Form (Personal Data)

REPRESENTATION BY ELECTED REPRESENTATIVE

A. – Elected Representative Details

Name: _____

Email Address: _____ Phone number: _____

B. – Representation Details

I have been asked to make representation on behalf of:

Name: _____

Address: _____

Any other unique information (if required) that will help in confirming the constituent's identity:

In relation to the following matter:

Please list any additional information you have attached to representation (if applicable)

C. – Request by a Third Party:

Where the request was not made by the constituent but by a third party e.g. family member on their behalf **please attach written consent** from the constituent or a statement (with supporting documentation) explaining why consent cannot be provided and why a representation is in their interest.

Please print name of person making request: _____

State relationship to the constituent: _____

D. – Elected Representative Declaration and Signature

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

Cllr./Deputy Mayor: _____ Signature: _____

Examples of unique information that would satisfy this requirement (if so required) are: driver's license or passport, or any other document that is currently accepted locally as proof of identity. However, this list is not to be considered exhaustive and preclude the submission of some other unique information that might satisfy the requirement.

Appendix 2 – Representation form involving the release of Special Category/ Sensitive

A. – Elected Representative's Details

Name: _____

E-mail address: _____ Phone no: _____

B. – Representation Details

I have been asked to make representations on behalf of:

Name: _____

Address: _____

Any other unique information (if required) that will help in confirming the constituent's identity:

In relation to the following matter:

Please list any additional information you have attached to representation (if applicable):

Notice to Constituent/Data subject

To find out how your personal data stored and managed by the elected member making this representation on your behalf please see their privacy statement. Please note that if you contact details change after you ask for this representation to be made you should notify the change in your details to the elected member who made the request.

¶

C. – Consent to Provide Special/ Sensitive Personal Data (where necessary)

I consent to the above named elected representative being provided with my special/sensitive data by: _____

Council where this is necessary for the purpose of a response to this representation: _____

Constituent name: _____ Signature: _____

5. Examples of unique information that would assist this requirement (if so required) are: driver's license or passport; or any other document that is commonly accepted locally as proof of identity. However, this list is not to be considered exhaustive and include the submission of some other unique information that might assist this requirement.

¶

D. – Request by a Third Party

Where the request was not made by the constituent but by a third party e.g. family member on their behalf please attach written consent from the constituent or a statement (with supporting documentation)⁵ explaining why consent cannot be provided and why a representation is in their interests

Print name of person making the request: _____

State relationship to constituent/data subject: _____

¶

E. – Elected Representative Declaration and Signature

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

¶

Name of Council I/ro/Deputy/Senator: _____

Signature: _____

¶

IN TODAY'S TRAINING...

Overview of GDPR

**Seven Principles of
Data Management**

Data Subject Rights

For Elected Representatives



Office Management

Campaigning

Making Representations

CONCLUSIONS

- The purpose of GDPR is to protect our privacy by protecting our personal data. ‘Do unto others’
- Elected members are DATA CONTROLLERS and in an elected position of trust. You need to understand your obligations as outlined and must:
 - Adhere to principles relating to processing of personal data
 - Understand and uphold obligations as a data controller
 - Uphold rights of data subjects
- The key role of elected representatives is recognised in Data Protection Act 2018 which provides the legal basis for:
 - Use of personal data for political campaigning purposes – this is in the public interest
 - Processing of personal data to make representations
- Read the DPC Guidance as DPC is responsible for enforcement
- Guidance provided by LGMA but need to understand how this will work in your Council
- **GDPR is here to stay!**

CONTACT DETAILS

Gerry Egan Consulting

gerry@gerryegan.ie

086 2591409

Consulting | Training | Advice | Implementation