



# Data Subject Rights Under GDPR

FERGAL CREHAN BL

DATA PROTECTION OFFICER, THREE IRELAND

# Subject Rights Under GDPR

## ▶ Chapter III:

Article 12 – Transparency and Modalities

Article 13 – Information

Article 14 – Information (3<sup>rd</sup> Parties)

Article 15 – Access

Article 16 – Rectification

Article 17 – Erasure

Article 18 – Restriction

Article 19 – Notification

Article 20 – Portability

Article 21 – Object to processing

Article 22 - Automated Decision Making

Article 23 - Restrictions

# Transparency & Modalities

- One Month (extendable by two months)
- Controller may request information to confirm the identity of the data subject
- No fee for most requests
- Where requests “manifestly unfounded or excessive, in particular because of their repetitive character” a fee may be charged or the request may be declined
- Controller must prove manifestly unfounded or excessive character of requests
- Information should be concise, transparent, intelligible and easily accessible
- Clear and plain language, in particular for any information addressed specifically to a child

# Right to Information

- Right to information about the controller, the data processed, purposes, etc
- Where data obtained from 3<sup>rd</sup> parties, information regarding the source
- Legal Basis must be cited for each type of processing
- Privacy Statement should satisfy this requirement pro-actively
- Article 5.1 (a) – Data must be “processed lawfully, fairly and in a transparent manner”

# Privacy Policies, Notices & Statements

- Privacy or Data Protection *Policy* is an internal document
- Privacy *Statement* is public-facing
- Privacy Statement should be separate from general Terms & Conditions
- “Layered Notice” – short Privacy Notice links to full Privacy Statement
- Some types of processing should have their own Privacy Statements (e.g. job applicant, CCTV, website & cookies)

# Right of Access

- Where request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
- Shall not adversely affect the rights and freedoms of others i.e. redaction may be required.
- Guidance from ODPC remains valid here, e.g. re CCTV footage

# Right to Rectification

- Supplements Article 5(1)(d): Personal Data shall be “accurate and, where necessary, kept up to date
- Is an on-demand right (Article 5(1)(d) is a positive obligation)
- Includes right to have incomplete data supplemented
- Organisations should have an administrative process in place to update records on demand (e.g. change of address, change of name)

# Right to Erasure

- ▶ “Right to be Forgotten” is not a new right – merely a right not to have data held in non-compliance with existing DP principles, eg:
  - Where no longer necessary for the purposes for which they were collected
  - Where consent has been withdrawn
  - Where data is unlawfully processed
- ▶ Can be refused where the data is held in compliance with GDPR
- ▶ A complete and properly implemented Retention Policy should pre-empt all Deletion Requests.



# Right to Restriction

- ▶ To partially or temporarily suspend processing of data:
  - Where accuracy is contested
  - Where processing is unlawful but subject chooses restriction over deletion
  - Where no longer needed for original process but held for purposes of a legal claim
  - Where a Legitimate Interest is contested
- ▶ Organisations should have the ability to take certain data out of production without fully deleting it (e.g. masking, retaining hard copy)
- ▶ Good compliance with core DP Principles should pre-empt restriction requests.

# Notification

- ▶ Controller shall notify Data Subject that a Deletion, Rectification, Erasure or Restriction Request has been processed
- ▶ Organisations should prepare template letters confirming or refusing such requests, and include notification as final step in the process.

# Portability

## ▶ Scope:

- The data must have been provided to the controller by the subject.
- The data must be processed on the basis of either consent or contract.
- The data must be processed by automated means.

## ▶ Not in scope:

- Records held on other bases, e.g. billing records held in compliance with tax law
- Unstructured data, hard copies – Not processed by automated means

# Portability

- ▶ Subject has right to receive the data directly
- ▶ Subject has right to have the data transferred to another controller “without hindrance”
- ▶ A “structured, commonly used and machine-readable format” – Excel .csv?

## **But:**

- ▶ No corresponding duty on a Data Controller to receive data
- ▶ Existing DP principles still apply
- ▶ No duty on Data Controllers to build interoperable systems

# Right to Object

- ▶ Right to Challenge a Legitimate Interest Basis
  - Ensure you minimise reliance on LI, carry our balancing exercise for LI, keep records. Perform DPIAs where necessary
- ▶ Right to Opt out of processing for Direct Marketing
  - Ensure not only your direct marketing lists, but all processing and profiling databases have opt out facility
- ▶ Right to Challenge Public Interest Processing
  - Ensure DPDD practices are in place, carry our DPIAs where necessary

# Automated Decision Making

- ▶ General Prohibition on Decisions based solely on automated processing which produce legal or similarly significantly effects, except:
  - Where necessary for entering into, or performance of, a contract
  - In accordance with EU or domestic law
  - On Consent
- ▶ Data controller shall implement suitable measures to safeguard the data subject's rights to:
  - Obtain human intervention
  - Express his or her point of view
  - Contest the decision

# Restrictions

- ▶ Article 23 provides that member states may restrict Data Subject Rights
- ▶ Data Protection Act 2018 restricts rights where necessary:
  - to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State.
  - prevention, detection, investigation and prosecution of criminal offences
  - administration of any tax, duty or other money due or owing to the State
  - in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings

# Restrictions

- For the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim
- For the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the controller in relation to the claim
- Opinions given in confidence on an understanding of confidentiality
- By Regulation for purposes of General Public Interest



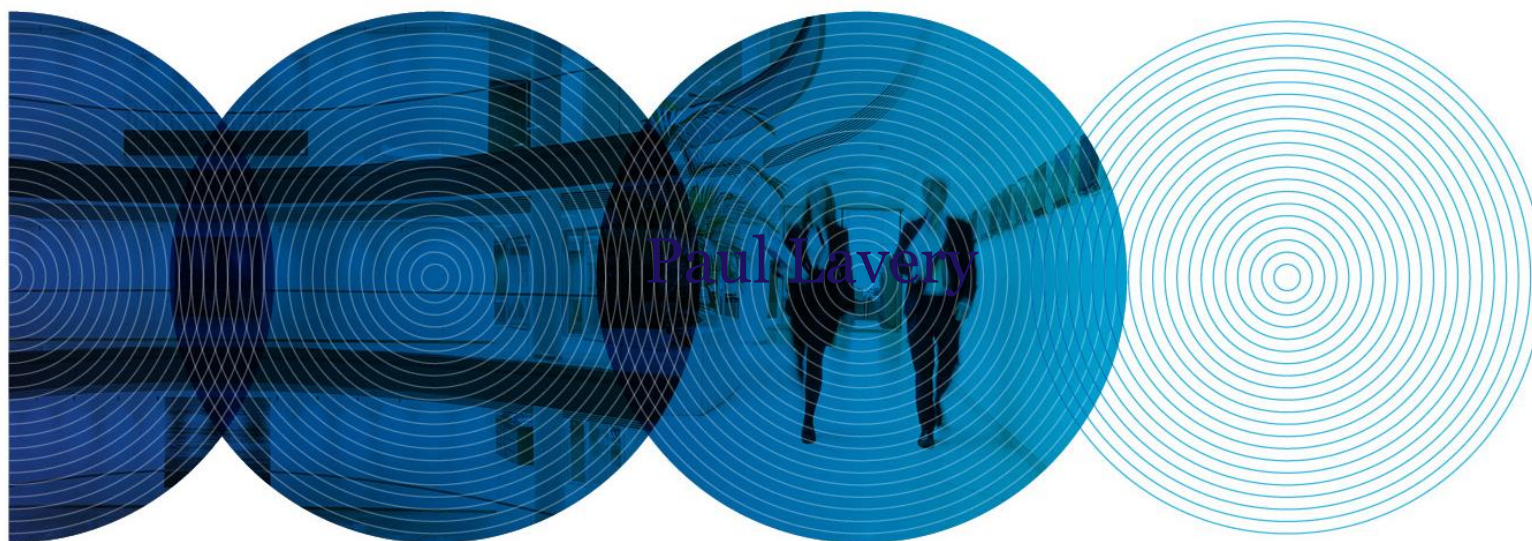
---

# GDPR: Effect of Data Protection reform on law firms and role of Law Society of Ireland

Paul Lavery, McCann FitzGerald

Saturday, 6 October 2018

MCCANN FITZGERALD



---

# Topics

- The EU Data Protection Regulation and Data Protection Act 2018 – Main Implications for Law Firms and Compliance Steps
- Role of Law Society of Ireland

---

# GDPR – Recap

- Replaced existing law in all member states on **25 May 2018**
- Designed to result in single, uniform set of data protection rules applying across the EU
- Retains and enhances existing data protection concepts and requirements
- Increases obligations on controllers/processors
- Affords new rights to data subjects
- GDPR represents an “evolution” of rights and obligations, but a “revolution” in respect of administrative compliance burden and sanctions for non-compliance
- Fines – Up to €20 million or 4% of annual worldwide turnover

---

# Legislative Regime

- General Data Protection Regulation
- Data Protection Act 2018
- Electronic Privacy Regulations 2011 (will ultimately be replaced by new ePrivacy Regulation)

---

# GDPR Compliance – Data Protection

- Why is data protection important to Law Firms?
- Holder of large repository of client data  
(particularly where law firm mainly acts for individuals rather than corporates)
- Affects clients – big compliance challenge –  
opportunity to advise on clients' GDPR obligations  
and compliance

---

# Main Data Protection Obligations – Similar to previous law

- **Fair and Transparent Processing** (*Information notices with details on use and disclosure of data and GDPR rights*)
- **Identifying a legal basis for processing** (*legitimate interests, consent, necessary for performance of contract etc*)
- **Keeping only for specified, explicit and lawful purposes**
- **Data minimisation** – only collecting and using data which is adequate, relevant and proportionate
- **Security** – *obligation to implement and maintain appropriate technical and organisational security measures.*

---

## Main Data Protection Obligations – Similar to previous law

- **Accuracy** – *appropriate steps to keep data accurate and up to date*
- **Record Retention** – *personal data not to be held for longer than necessary (appropriate retention and deletion policies)*
- **Subject Access Requests** – *providing copies of personal data to data subjects on request*
- **Transfer outside EEA** – prohibitions on transfers outside EEA – need to be able to rely on exemption such as consent, model clauses, EU/US Privacy Shield etc

---

# Main Data Protection Obligations (New)

- **Record of Processing Activities/Data Inventory** – *recording categories of data, categories of processing activities, categories of recipients, data transfers, retention times and security measures*
- **Documenting and Evidencing Compliance** – *Drafting and implementing relevant data protection policies and information notices; privacy by default and by design; data protection impact assessments*
- **Engaging Service Providers** – *Detailed data processing provisions required to be included in contracts*



---

# Main Data Protection Obligations (New)

- **Right of Erasure** – *right of data subject to deletion of data in certain circumstances*
- **Data Portability** – right to move copy data to another controller in certain circumstances
- **Data Protection Officers** – Potential need to appoint DPO
- **Security Breach Notifications** – mandatory notifications to DPC and affected data subjects in certain circumstances

---

# GDPR – Main Implications for Law Firms

- **Data Inventory** – *what, where, why and for how long* – need to carry out full inventory of personal data
- **Data protection policies and procedures** – review of any existing policies and procedures and potential need for additional policies
- **Controller/processor agreements** – will require more detail
- **Data protection notices/Privacy statements** – will require more detail
- **Data protection audits/assessments; Data Protection Impact Assessments** – new forms of processing are likely to require data protection impact assessments
- **Data security breaches** – mandatory reporting

---

## GDPR – Main Implications for Law Firms *cont'd*

- **Identify Lawful Basis for Processing** – Articles 6 and 9
- **DPO Appointment** – Need to consider whether there is a need to appoint DPO – Potential need to enshrine guaranteed independence in role
- Potential Fines “Ups Ante” in respect of compliance

---

# Record of Processing Operations/Data Inventory

- Article 30
- Record of Processing activities
  - Details of controller;
  - Categories of data subjects and personal data;
  - Purposes of processing;
  - Categories of recipients of personal data;
  - Transfers outside EEA;
  - Envisaged time limits on retention of personal data;
  - General description of security measures

---

# Notices and Policies

- Notices:
  - Data protection notice to clients
  - Data protection notice/privacy statement on website
- Policies
  - General DP Policy
  - Data Security Policy
  - Breach handling and notification policy
  - Retention/Deletion Policy
  - Other policies – access request; accuracy; right to be forgotten; data portability (could be included instead in one overall internal DP Policy)

---

# Appointing Service Providers (where they process data on your behalf)

- Article 28
- Use only processors providing sufficient security guarantees
- Processor not entitled to engage sub-processor without controller consent
- Requirement to have contract with processor which includes various provisions (more detailed than required under existing law), including:
  - processing in accordance with instructions;
  - Security measures;
  - Confidentiality obligations
  - Audits and inspections
  - Notification of data security incidents
  - Return or deletion of data on expiry of processing services

---

# GDPR – Internal Governance and Responsibility

- Increased internal governance and responsibility
  - removal of registration obligation (though law firms were already exempt from this requirement)
  - requirement replaced with obligation to adopt internal policies and procedures which demonstrate compliance with data protection laws
  - privacy by default and design
  - Data Protection impact assessments

---

# Identifying Appropriate Lawful Basis for Processing

- Personal data – Identify lawful basis under Article 6:
  - Consent
  - Performance of a contract
  - Legitimate interests
  - Compliance with legal obligation



---

# Identifying Appropriate Lawful Basis for Processing

- Special categories of personal data – Identify lawful basis under Article 9 and/or Sections 46 to 54 Data Protection Act 2018
  - Article 9 - Explicit consent
  - Article 9 - Processing necessary for compliance with employment or social security or social protection law
  - Article 9 - Processing necessary for establishment, exercise or defence of legal claims
  - Section 47 DPA – processing necessary for purpose of providing legal advice

---

## GDPR – Data Protection Officers

- Various entities will be required to appoint a data protection officer (“DPO”) to oversee compliance with the Regulation:
  - all public authorities (except courts)
  - Where core activities require regular and systematic monitoring of data subjects on a large scale
  - Where core activities consist of processing on a large scale of special categories of data and personal data relating to criminal convictions
  - other categories to the extent required by Member State law

---

# Data Protection Officer

- Role enshrined under GDPR (Chapter IV, Section IV)
- DPO – to be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil DPO tasks
- DPO may be employee or third party service provider
- Contact details of DPO must be published and notified to Data Protection Commissioner

---

## Data Protection Officer (cont'd)

- Need to ensure that DPO is involved properly and in a timely manner in all issues relating to protection of personal data
- DPO must be provided with appropriate support and resources (internal and external support and legal advice)
- DPO must be independent (cannot receive instructions from employer regarding exercise of DPO functions)
- DPO cannot be dismissed or penalised for performing DPO tasks
- DPO shall report to highest management levels
- DPO may fulfil other tasks provided that the other tasks do not result in conflict of interest

---

# DPOs

- Law Firms need to consider whether to appoint DPO
- GDPR and associated guidance unclear
- Some law firms – particularly firms engaging in core activity of large scale processing of criminal data (e.g. criminal defence law firms) or large scale processing of health data (personal injury law firms) are more likely to need to register
- Other firms – potentially exempt

---

# GDPR – Compliance Steps

1. Get senior “buy in” to DP compliance – without senior buy in, compliance will be hard to achieve
2. Data Inventory – Review/health check of data and processing activities – data protection audit/assessment
3. Review basis for processing – *eg* consent, legitimate interests, necessary for contract performance *etc*
4. Policies, procedures and notices – review/develop necessary internal policies/procedures and notices

---

# GDPR – Compliance Steps for Clients

5. DPO appointment (where necessary)
6. Review third party processing and international transfers
7. Keep an eye out European Data Protection Board and DPC guidance

---

# Role of Law Society of Ireland

- Will provide guidance to law firms on data protection compliance
- Has published, via IP and DP Law Committee, suggested compliance documentation:
  - GDPR FAQs
  - GDPR - steps to compliance
  - GDPR Subject Access Request guidance and checklist
  - Data sharing protocol with Bar Council
  - Template data protection/privacy notices – website notice, client notice and employee notice
  - Template record of processing activities



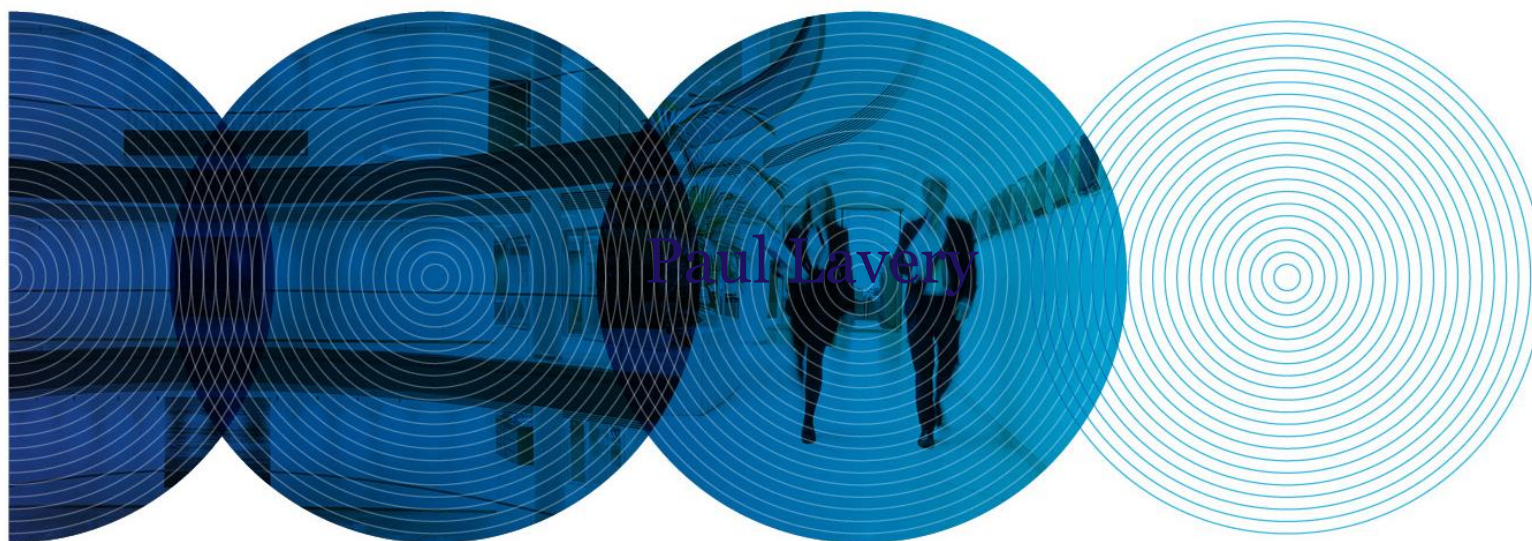
---

# GDPR: Effect of Data Protection reform on law firms and role of Law Society of Ireland

Paul Lavery, McCann FitzGerald

Saturday, 6 October 2018

MCCANN FITZGERALD



# Data Protection Rights: Roots and Reasons

Simon McGarr

mc | garr  
SOLICITORS



# HELLO!

**I am Simon McGarr,**

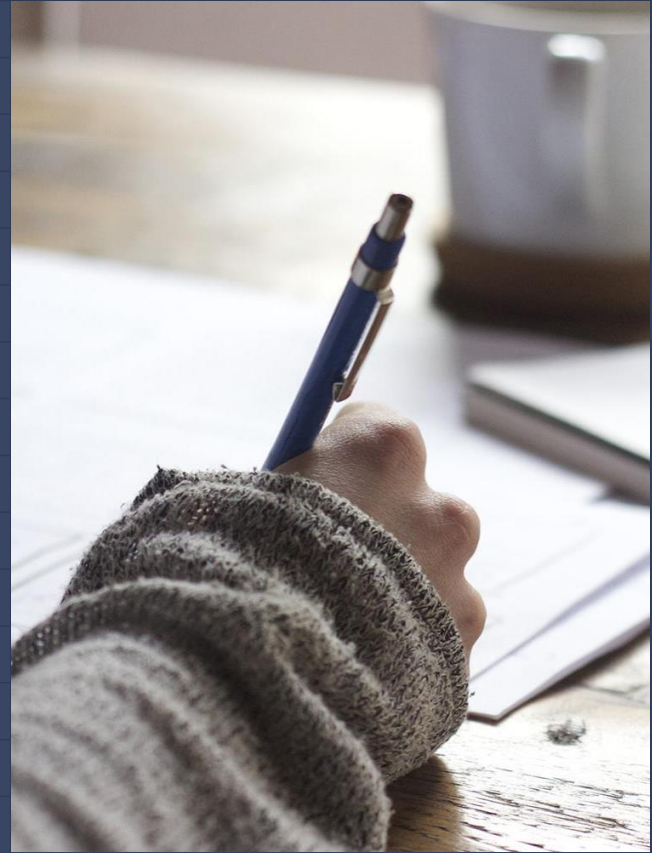
Solicitor and Consultant

You can find me at

[mcgarrsolicitors.ie](http://mcgarrsolicitors.ie)

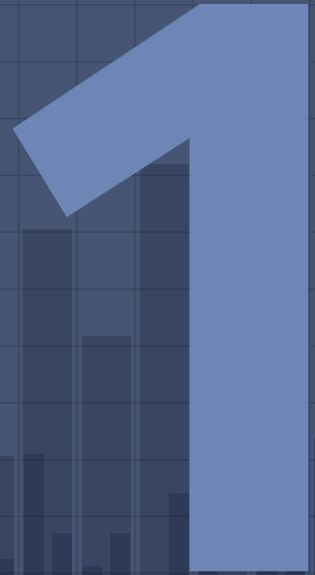
[Datacomplianceeurope.eu](http://Datacomplianceeurope.eu)

@Tupp\_ed on Twitter



# Roots of Data Protection Rights

Some history and context



# Data Rights Are Human Rights

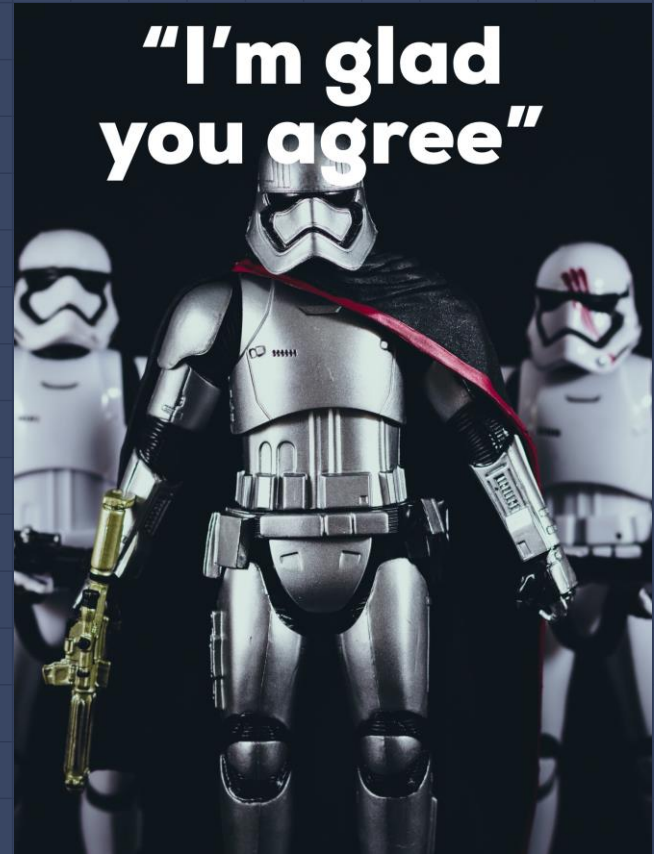
## **Universal Declaration on Human Rights (1946-48)**

*"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"*

Data Protection Grew  
out of Privacy

## European Convention on Human Rights (1949-50)

*"Everyone has the right to  
respect for his private and  
family life, his home and his  
correspondence."*



# EU Data Protection Right is distinct

## **EU Charter of Fundamental Rights**

### Article 8

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

Bunreacht is a living document

1937:

**Article 40.1, Bunreacht na hÉireann**

**“The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law.”**







# 2016:

*“One might accordingly ask how the dwelling could in truth be a “place of repose from the cares of the world” if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.”*

– Hogan J, Schrems v DPC (No.1)

# Giving rights their form

Specific powers of the individual granted by the GDPR and Data Protection Act



2

# Data Subject Access Requests

- Can ask for a copy of any data, held in any form (documents, computer files, emails, CCTV) held by an organisation on them
- Organisation must comply within a month.

# Real Consent

Consent not valid unless

- Freely Given
- Specific to the use
- Informed
- Unambiguous
- Easily withdrawn



# Consent but for a Specific Purpose

## **Specific Consent**

Know what use the data will be put to.

State that clearly.

Use it only for that purpose.

**Vs**

## **Function Creep**

Collect data for one purpose but then start using it for one or more extra purposes.

Never say

“I wonder what else we could do with this?”

# Information about processing

## Who and why

- (i) the controller's identity,
- (ii) the purpose of each of the processing operations for which consent is sought,

## What and how

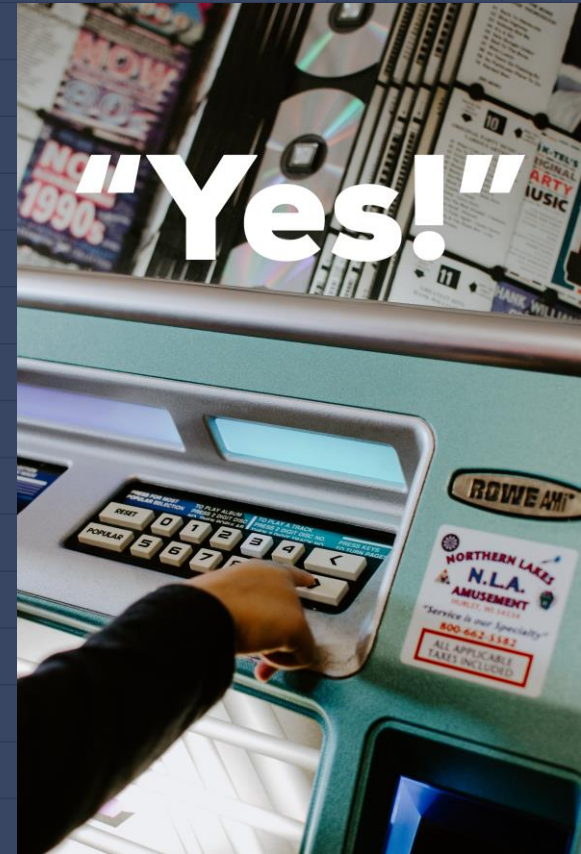
- (iii) what (type of) data will be collected and used,
- (iv) the existence of the right to withdraw consent,

## Where and how

- information about the use of the data for automated decision-making
- on risks and safeguards of data transfers in the absence of an adequacy decision

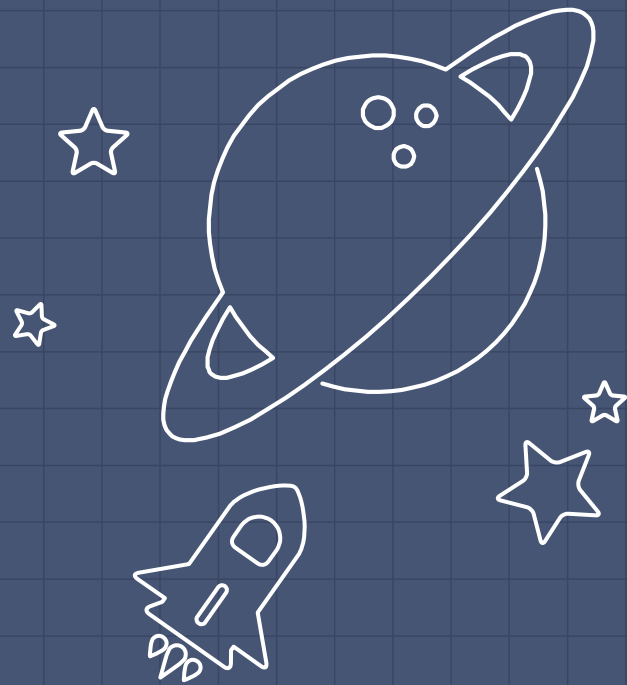
# Unambiguous Consent

The individual has to take a specific and clear step to indicate their consent.



# Withdraw Consent

Should be as easy to say No as it was/is to say Yes





# Reasons: Why it all matters

Data Protection is no abstract right



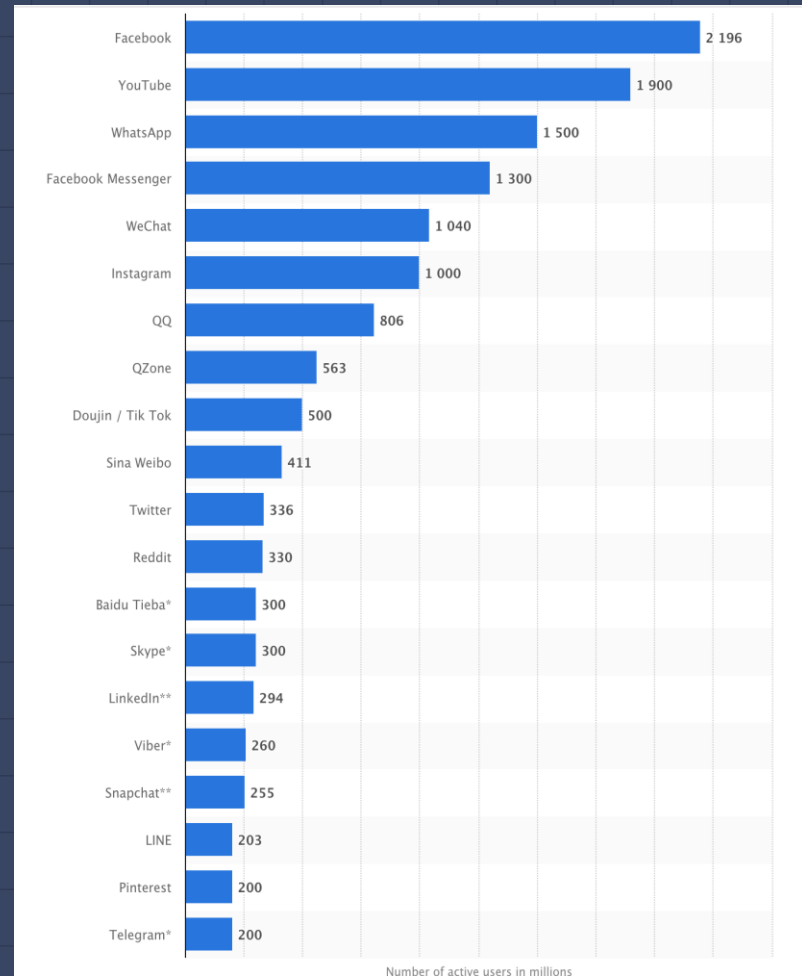
3

# Ireland has a particularly key role to play



# A sense of scale

Social Media operates on a scale without any parallel. Each of the top 4 platforms have more active users than the entire Catholic Church. (1.2bn, per the Vatican).

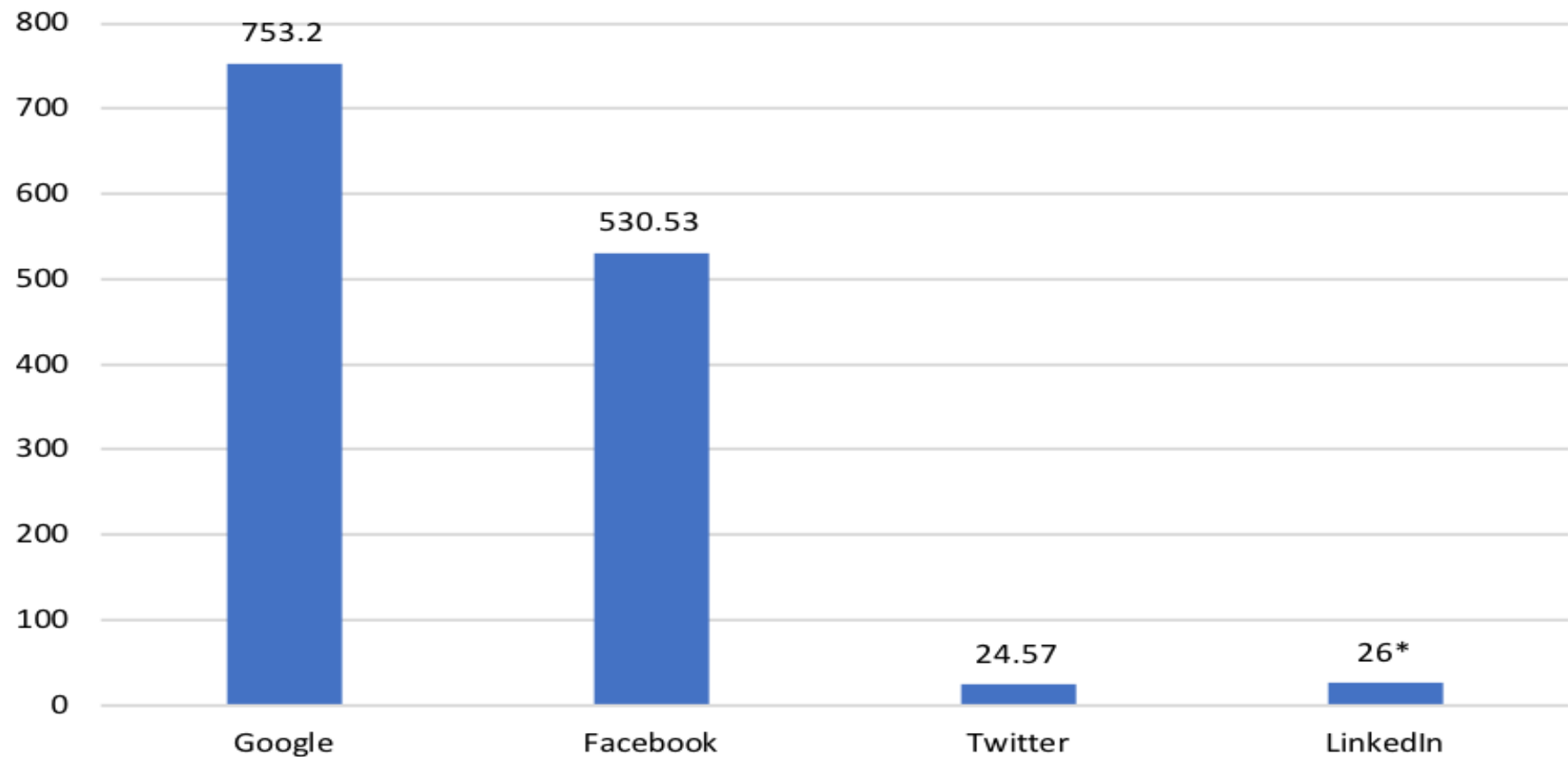



# 2,240,000,000

That's 2.24 billion active Facebook users, Q2 2018



## Market Capitalisation in Billions of US\$





The vast income streams of Social Networks rely on a continued, and -ever expanding- ability to profile individuals and to then sell advertising against the knowledge about people gained through that surveillance

If you're not paying for a product, you are the product.



# THANKS!

## Any questions?

Creative Commons Photo Credits:

- Surveillance Chic by Ryan McBride
- CJEU Grand Chamber: Simon McGarr





# The Role of the Data Protection Commission

Karen Gallagher  
Senior Associate  
Pinsent Masons (Ireland)



# Agenda

- Background
  - Public Awareness
  - Resources
  - Importance
- Role of the DPC under GDPR
  - Independent status
  - Competence, tasks and **powers**
  - **Role as a LSA** & co-operation between SAs
  - Role on the EU Data Protection Board

Part 1

# BACKGROUND

# Background

- Data Protection Commission - established under Data Protection Acts 1988 to 2018
- Formerly- ODPC – s14, s20, s62, s63 & s15(4) DPA 2018
- Supervisory Authority under GDPR ((EU) 2016/679) and Law Enforcement Directive ((EU) 2016/680)
- Chapters VI and VII GDPR
- Parts 2 and 6 of the DPA 2018

# Public Awareness

- Public Awareness Survey 2013 - 65% awareness of the office, compared to 25% in 1997
- In 1997, only 2% of respondents spontaneously mentioned the Office when asked to name organisations dealing with privacy complaints
- 2017 Annual Report – 79% increase in complaints from previous year, 69% increase in queries, 25% increase in valid data breach notifications, 4 million twitter impressions.

# Resources

- Staff numbers
  - 7 staff – 1997
  - 85 staff- 2017
  - 55 new hires for 2018
  - Capacity to appoint up to 3 Commissioners (s15(1))
- Budget
  - £313,565 - 1997
  - €7.5m - 2017
  - €11.7m- 2018

# Importance

- International Significance
  - Multinational tech companies have EMEA HQ in Dublin – LSA
  - Brexit
- Powers
  - Increased fines
  - Powers of authorised officers
    - Reasonable assistance re operation of data equipment
    - Attendance before authorised officers to provide relevant information/answer questions
  - Mandatory notification of data breaches to DPC (Art 33)
  - Requirement for companies to report

Part 2

# ROLE OF THE DPC UNDER GDPR



# Independent Status

- Chapter VI, Section 1 GDPR
- Art 51- Establishment
- Art 52 – Independence
  - Must act with complete independence
  - Free from external influence
  - Choose own staff
  - No actions incompatible with duties
  - Financial control that does not impact independence
  - Obligations on MS to ensure sufficiently resourced- human, technical, financial, premises, infrastructure

# Independent Status

- Art 53- Conditions for Members
  - Transparent appointment procedures
    - S15(3) DPA 2018 - Government appoints Commissioner on recommendation of Public Appointments Service
  - Qualifications, experience and skills required
  - Dismissal - serious misconduct or no longer fulfils the conditions required
- Art 54 – Member State Law to provide for:
  - Rules on establishment, appointment, eligibility etc (s10, s15 DPA 2018)
  - Duty of Professional Secrecy (s26, s27 DPA 2018)

# Competence

- Chapter VI, Section 2 GDPR – Competence, tasks & powers
- Art 55- Competence
  - Within territory of Ireland –
    - Recital 122 – in Ireland or targeted at DS in Ireland
  - Public authorities & private bodies acting on basis of a legal obligation, in the public interest, or exercise of official duty
  - No competence – processing by courts acting in judicial capacity (Chief Justice- s157 2018 Act)

# Competence - LSA

- Art 56 – Competence of Lead Supervisory Authority
  - Primary responsibility for cross-border data processing activity
  - Co-ordinate investigation, involving other “concerned” SAs
  - LSA = SA of the main or single establishment of the controller or processor
  - Recital 36 - “main establishment”
    - Central administration
    - Decisions on processing (DC)/Where processing happens (DP)
  - DPC = LSA for tech cos, pharma, multinational companies

# Tasks - Overview

- Art 57- Tasks
  - 22 specified tasks set out
  - No 22 - “fulfill any other tasks related to the protection of personal data”
  - Facilitate complaints – eg by providing complaint form
  - Free of charge for DS and DPOs.
  - But- if manifestly unfounded or excessive-reasonable fee for administrative costs

# Tasks – Key Tasks

- Monitor and enforce application of GDPR
- promote awareness and understanding among public, and controllers & processors
- Assist data subjects, deal with and investigate complaints & conduct investigations
- Co-operate with other supervisory authorities & contribute to activities of EU Data Protection Board
- Monitor development of technical and commercial practices
- Encourage development of codes of conduct and certification systems & draft and publish criteria for accreditation
- Authorise contractual clauses and approve binding corporate rules

# Powers - Overview

- Art 58 GDPR
  - Investigative powers
  - Corrective powers
  - Authorisation and advisory powers
  
- Part 6 DPA 2018
  - Ch 2 – Enforcement of GDPR
  - Ch 4 – Inspection, Audit & Enforcement
  - Ch 5 – Investigations
  - Ch 6 – Administrative Fines
  - Ch 7 – s147 Prosecution of summary offences by DPC

# Investigative Powers

- Art 58 (1) Investigative Powers include:
  - Order DC or DP to provide information –  
(s130(1)(c) production of documents; s130(2) access to equipment; s131 search warrant; s132 information notices; s135 reports; s138(1), (3) production of documents and attendance before authorised officers to answer questions)
  - Data Protection Audits (s 136)
  - Obtain access to personal data & all information necessary to perform tasks (ss130-132, s135, s138)
  - Access to premises, equipment and means of processing (s130)



# Failure to Co-operate

- With an AO re an inspection (s130(7))
- With a reviewer re a report (s135(15))
- With an AO re an investigation (s138(12))
  - Offence –
    - Summary - Class A fine/12 months imprisonment
    - Indictment – €250k fine/5 years imprisonment
  - S138(4),(5) court order to compel compliance with request to produce documents/answer questions from investigator

# Corrective Powers

- Art 58 (2) Corrective Powers include:
  - Order DC/DP to comply with DS request (s109 (5)(d); s133)
  - Order DC/DP to bring processing operations into compliance (s115; s 133)
  - Order DC to communicate data breach to DS (s109 (5)(d); s133)
  - Impose limitations (including bans on processing) (s134)
  - Order rectification, erasure, restriction of processing (s109 (5)(d); s133)
  - Impose administrative fines €€€ (s141)

# Authorisation and Advisory Powers

- Art 58(3) Authorisation and Advisory Powers include:
  - Advise DC using prior consultation procedure
  - Issue opinions on data protection issues
  - Authorise processing for tasks carried out in public interest
  - Provide opinion on and approve draft Codes of Conduct
  - Accredit certification bodies, issue certifications & approve certification criteria
  - Adopt standard data protection clauses re data processing and transfers to third countries/international organisations
  - Authorise contractual clauses
  - Authorise administrative arrangements
  - Approve binding corporate rules

# Powers – Member State Law

- Art 58 (4) Safeguards on powers – effective judicial remedy and due process
  - DPC must apply to Circuit Court to confirm fine (s143)
  - Appeals
    - Decision to impose fine (s142)
    - Information notice or enforcement notice (s150(1))
    - DS or person affected appeal of decision (s150(5))
    - DS appeal of DPC failure to deal with complaint (s150(7))
    - Right of further appeal on point of law (s150(11))
  - Privileged material (s151)
  - Statements or admissions made during investigation (s138(8))

# Powers – Member State Law

- Art 58(5) Power to bring infringement to attention of authorities, commence or engage in legal proceedings
  - Prosecution of summary offences (s147)
  - Search warrants (s131)
  - Application to High Court for determination re adequate level of protection (s163)
- Art 58 (6) Any additional powers
  - All such powers as are necessary or expedient for the performance of its functions (s12(5))

# Co-operation

- Chapter VII - Art 60- Co-operation and consistency between LSA and CSA
  - Concerned Supervisory Authorities (CSA) can be involved where establishments in their MS, DS substantially affected in their MS, or they receive a complaint. LSA must co-operate with them.
  - Other SAs can also deal with purely local cases.
- Art 61- mutual assistance
- Art 62 – joint operations (investigations, enforcement)

# Consistency

- Art 63 – SA to co-operate using consistency mechanism
- Art 64- Opinion of the Board – draft decisions of DPC on standard contractual clauses, binding corporate rules, codes of conduct etc.
- Art 65- Dispute Resolution by the Board where:
  - LSA rejects objection by CSA
  - Disagreement as to who is the LSA
  - SA fails to seek opinion or fails to comply with it
- Art 66 – Urgency Procedure – can't wait for board opinion
- Art 67- Exchange of Information - electronically

# EU Data Protection Board

- Arts 68 -76 – European Data Protection Board
  - SAs, EU Data Protection Supervisor and Commission (no voting right). Independent Secretariat
  - DPC must contribute
  - Tasks (Art 70)
    - Advise the Commission
    - Promote co-operation and consistent application of GDPR
    - Issue guidelines, recommendations, statements of practice.
  - Conciliate and determine disputes between SAs



# Questions?

Thank you!

Pinsent Masons (Ireland) is a general partnership regulated by the Law Society of Ireland. It is an affiliated entity of Pinsent Masons LLP, a limited liability partnership registered in England and Wales (registered number: OC333653). Reference to "Pinsent Masons" is to Pinsent Masons LLP and/or one or more of the affiliated entities that practise under the name "Pinsent Masons" as the context requires. The word "partner", used in relation to Pinsent Masons refers to a member or an employee or consultant of the partnership or any affiliated firm, with equivalent standing. A list of members of Pinsent Masons, those non-members who are designated as partners, and non-member partners in affiliated entities, is available for inspection at our offices or at [www.pinsentmasons.com](http://www.pinsentmasons.com). © Pinsent Masons.

For a full list of the jurisdictions where we operate, see [www.pinsentmasons.com](http://www.pinsentmasons.com)



# GDPR: key concepts & challenges

---

Emerald de Leeuw LL.B LL.M MSc

[Emerald@eurocomply.com](mailto:Emerald@eurocomply.com)



# Good morning!

---

Today we will cover:

1. Why was the GDPR introduced
2. Personal data & sensitive data
3. The data protection principle & how to actually comply with them
4. Children, Consent and ISS
5. Key considerations in operationalising compliance.



# EU Data protection reform

---

**1. Data became the new currency.** The right to data protection is a fundamental right in the European Union and control and surveillance of every communication online is incompatible with "*with Europe's fundamental values or our common understanding of a free society*".



**2. One set of rules** to resolve the fragmented legal landscape

**3. Territorial scope** to ensure the same rules apply to all businesses providing services to EU residents. Non-European companies, when offering services to European consumers, will have to apply the same rules and adhere to the same levels of protection of personal data.



# Personal Data v Sensitive Data

---

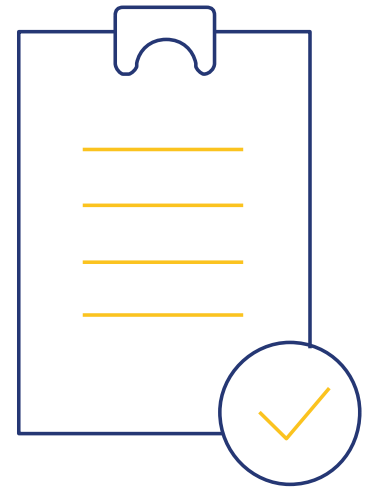
## Personal Data (art. 4(1) GDPR)

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;

## Special categories of data (art. 9(1) GDPR)

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

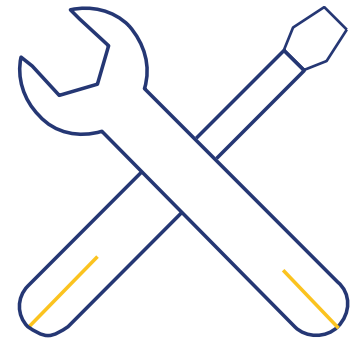


# Data Protection principles

---

## Adherence to the Data Protection Principles:

- a. Processing must be Lawful, Fair and Transparent
- b. Only for specific pre-defined purposes
- c. Data Minimisation
- d. Accuracy
- e. Storage Limitation
- f. Take 'appropriate measures' to ensure Integrity and confidentiality (Article 5(1))



## Accountability

The controller is responsible for and must be able to demonstrate compliance with the above principles. (Article 5 (2))

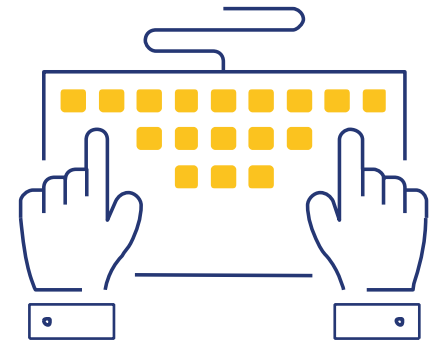
# What does that look like?

---

Requirement to register with your governing data protection authority is gone. Instead, you must prove you are doing the right thing. Compliance becomes process and documentation driven.

## “Appropriate organisational and technical measures”

1. Comprehensive record-keeping obligations
2. Appointing a DPO
3. International transfer mechanisms (BCR, Model Clauses etc.)
4. Privacy by Design/ Privacy by Default
5. Data Protection Impact Assessments
6. Security Measures





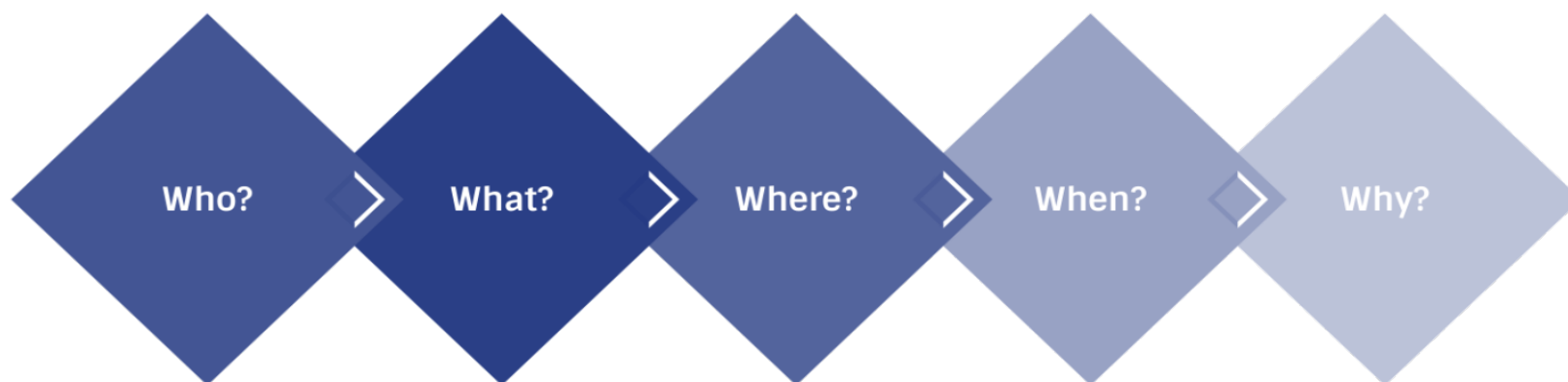
# Records of processing (art. 30 GDPR)

---

An overview of all the data your organisation processes.

Exemption for organisations with less than 250 employees **unless** the processing it carries out is

1. likely to result in a risk to the rights and freedoms of data subject, **or**
2. the processing is not occasional, **or**
3. the processing includes special categories of data or personal data relating to criminal convictions and offences.

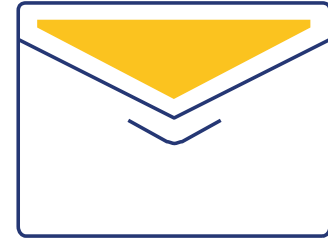


# 1. Lawful, fair & transparent

---

## Lawfulness

- Have an appropriate lawful basis for processing
- For special categories of data or criminal offence data, a special bases for processing
- Not using data for unlawful grounds



## Fairness

- Consider how processing may affect data subjects and be able to justify adverse impact
- Process data only in ways data subjects would reasonably expect

## Transparency

- How do transparency and accountability intersect?
- Notice v policy
- How to demonstrate transparency?
- What is a layered privacy notice and why is this a good idea?



## 2. Purpose limitation

---

**You need to specify your purpose or purposes for processing personal data in the records.**

**So what if you want to use the personal data for another purpose later on?**

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

**What is compatible? Consider the following:**

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and **what they would reasonably expect;**
- the nature of the personal data – e.g. is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - e.g. encryption or pseudonymisation.

# 3. Data minimisation, Accuracy & Storage limitation

---

## **Data minimisation**

- only collect personal data we actually need for our specified purposes.
- Periodically review the data and erasure when there is no longer a purpose.

## **Accuracy**

- Ensure data is correct and not misleading
- Update data where required
- Carefully consider any challenges to the accuracy of personal data.

## **Storage limitation**

- Be aware of what personal data is held and why we need it.
- It is vital to have appropriate retention periods for each category of data
- Ensure there is a process for execution if it's not automated
- Clearly identify if data is retained for public interest archiving, scientific or historical research, or statistical purposes

## **Data Integrity**

Appropriate security measures in place to protect the personal data. This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

# Children & GDPR

---

- Adherence to all principles
- Privacy by design & default
- Appropriate language
- Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child. Some services just raise the age for use of the platform i.e. the service isn't designed for kids. This means children do not have to seek parental consent at all. The onus is on parents to make sure that their children aren't using the service if they are underage.
- What about Information Society Services (ISS) and consent?
- Irish age for consent set to 16
- When offering ISS to a child, you need parental consent (or consent from the legal guardian) this again, must be auditable

# What is an ISS? (Article 1(1)(b) of Directive (EU) 2015/1535)

---

“any service normally **provided for remuneration**, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

**(i) ‘at a distance’** means that the service is provided without the parties being simultaneously present;

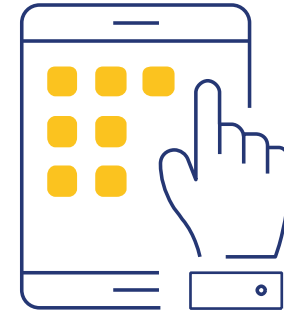
**(ii) ‘by electronic means’** means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

**(iii) ‘at the individual request of a recipient of services’** means that the service is provided through the transmission of data on individual request.”

# Children, consent & ISS

---

Most online services are ISS, even if the 'remuneration' or funding of the service doesn't come directly from the end user. **For example a social media company provided free to the end user but funded via advertising still comes within the definition of an ISS.**



It generally includes websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads.



# Lawful basis: personal data

---

**Consent** - The individual has given consent to the processing for one or more specific purposes. Consent will be harder to obtain under GDPR and needs to be “freely given, specific, informed and unambiguous” and a clear affirmative action is required. Can be withdrawn & triggers right to erasure

**Necessary for performance of a contract** - The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering into a contract. Triggers data portability right

**Legitimate interests** - The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Triggers right to object and additional requirements for privacy notice

**Legal obligation** - The processing is necessary for compliance with a (EU or Member State) legal obligation to which the controller is subject

**Vital interests** - The processing is necessary in order to protect the vital interests of the individual or of another natural person (i.e. medical emergencies)

**Public functions** - The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller



# Lawful basis: sensitive data

---

**Explicit consent** - The individual has given explicit consent. Derogations available for member states.

**Legal obligation related to employment** - The processing is necessary for a legal obligation in relation to employment and/or social security law or for a collective agreement.

**Archiving and Research** - The processing is necessary for archiving, scientific or historical research purposes or statistical purposes and is based on EU or Member State law.

**Legal claims** - The processing is necessary for the establishment, exercise or defence of legal claims or for Courts acting in their judicial capacity.

**Public information** - The processing relates to personal data which is manifestly made public by the data subject.

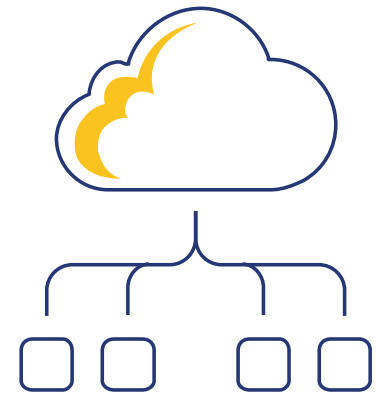
**Substantial public interest** - The processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law.

**Vital interests / Healthcare and Public Health** - The processing is necessary in order to protect the vital interests of the individual or of another natural person. (i.e. medical emergencies). The processing is necessary for healthcare purposes and is subject to suitable safeguards or the processing is necessary for public health purposes.

# Vendor management

---

- Non-compliance can lead to loss of business and companies are now responsible for ensuring compliance across all links in their supply chain
- **If you are a vendor to someone, you are exposed.**
- All relationships between data controllers and processors must be governed by a contract. The terms are stipulated by GDPR. (art. 28)  
Usually the most time-consuming elements of the documentation requirements
- **Remember: even if you don't care about your data supply chain, in B2B sales you will be asked. If you're non-compliant you are not going to remain on the approved vendor list.**



Thank you!

[emerald@eurocomply.com](mailto:emerald@eurocomply.com)



**EUROCOMPLY**

