An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

Brightwater TakeControl

General Data Protection Regulation (GDPR)

"Knowing the Basics"

Brightwater Recruitment - Dublin
28 June 2017

John Keyes LLB, BL
Assistant Commissioner & Head of Investigations
Office of the Data Protection Commissioner

@DPCIreland

Constitution of Ireland

Right to Personal Privacy under Article 40.3.1 *…The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens*

Court Interpretation: '*the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State'* [Hamilton P. in *Kennedy v. Ireland* [1987] IR 587]

Current Legal Position

- **Data Protection Directive 95/46/EC**
- **Data Protection Acts 1988 & 2003**
- **Electronic Privacy Directive 2002/58/EC; 2006/24/EC; 2009/136/EC)**
- **EC Electronic Privacy Regulations 2011 (SI 336/2011)**

Charter of Fundamental Rights of the European Union

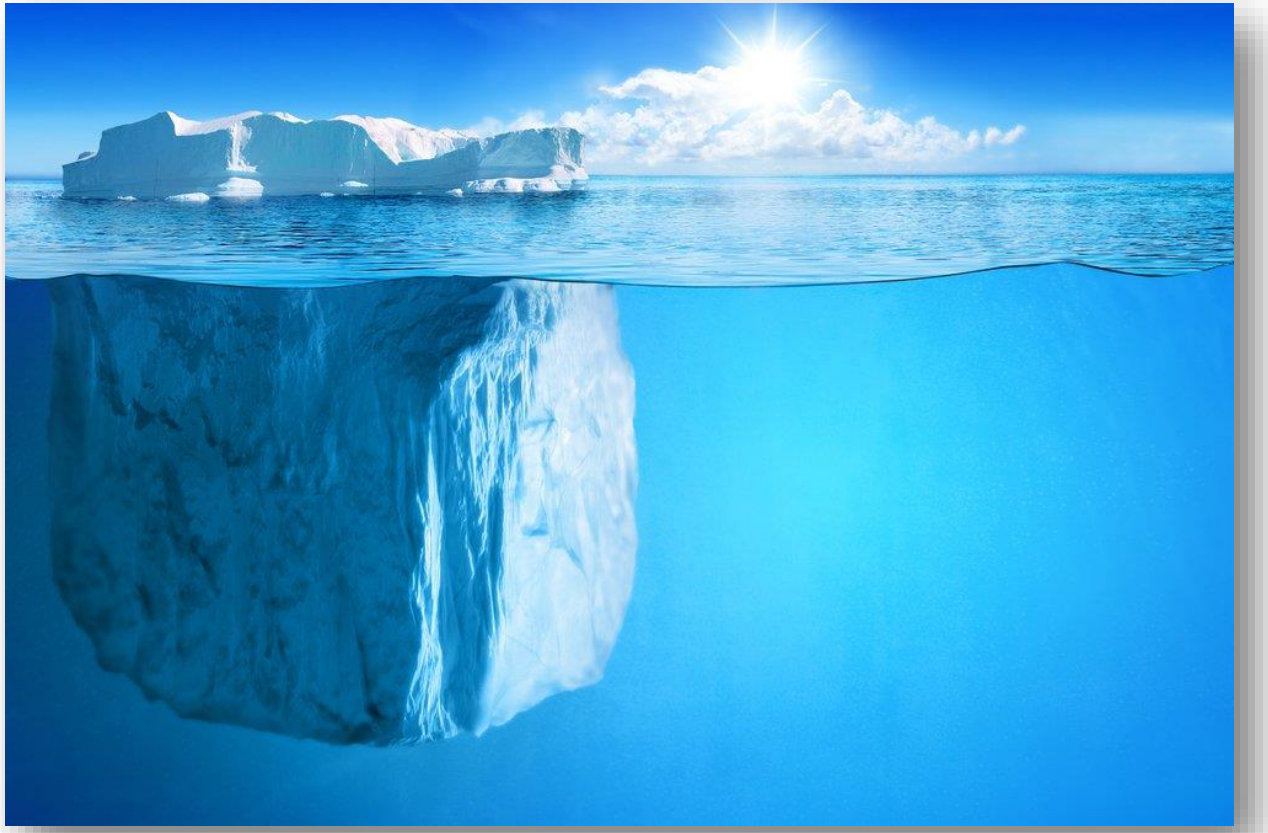
Article 8 - Protection of Personal Data

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.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

Impact of the Charter

- *Digital Rights Ireland*
- *Schrems*
- *Weltimmo*
- *Bara*
- *Costeja (Google Spain case)*

New Legal Position (from 25 May 2018)



Dead Ahead!

- General Data Protection Regulation (GDPR)
- Data Protection Bill
- E-Privacy Regulation

Brightwater
TakeControl

Countdown
to

G D P R

25th May 2018

GDPR

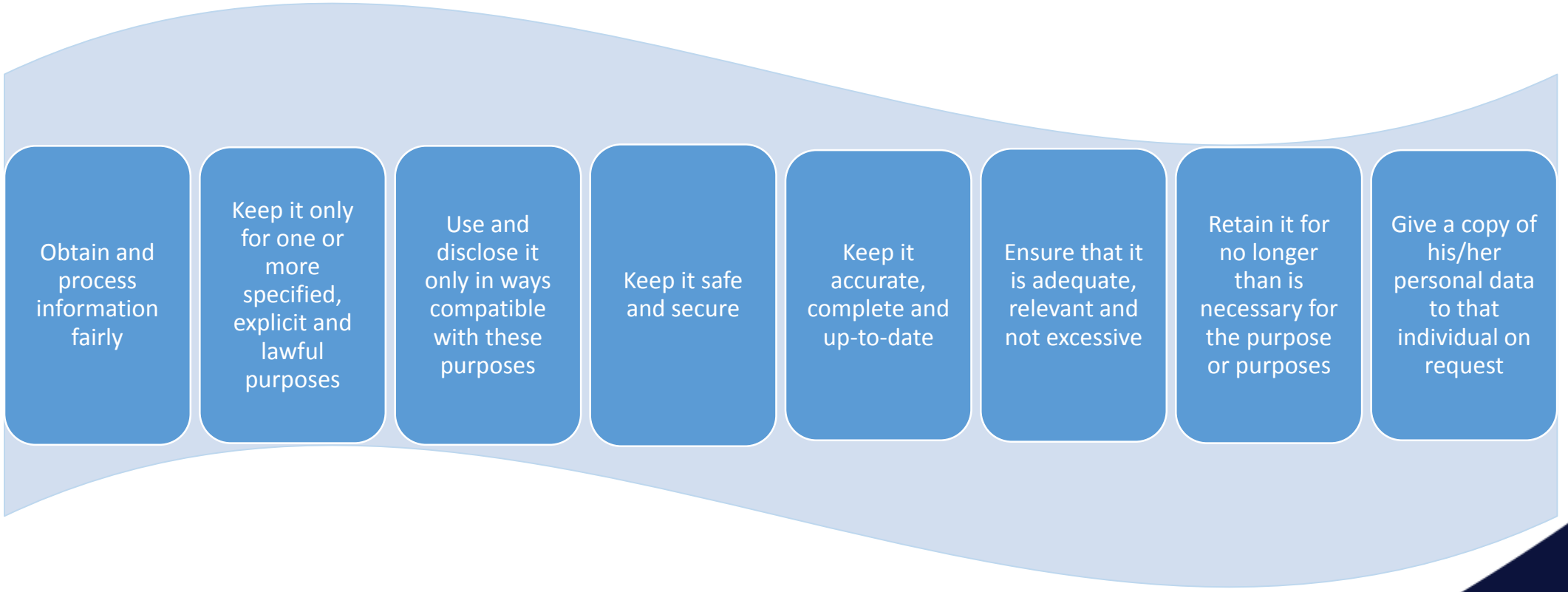
- 173 Recitals (not having force of law)
- 99 Articles (having full force of law)

GDPR – Recital 4

"The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"

"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties"

The 8 Principles of Data Protection

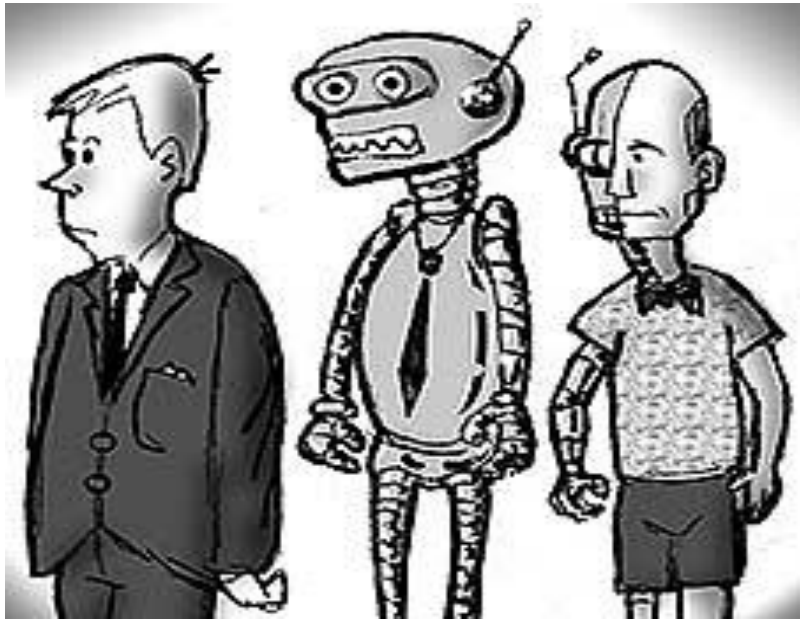


Personal Data

- Data from which the data subject can be identified
- Data which relates to the data subject

GDPR Definition of Personal Data (Article 4.1)

- any information
- relating to
- an identified or identifiable
- natural person



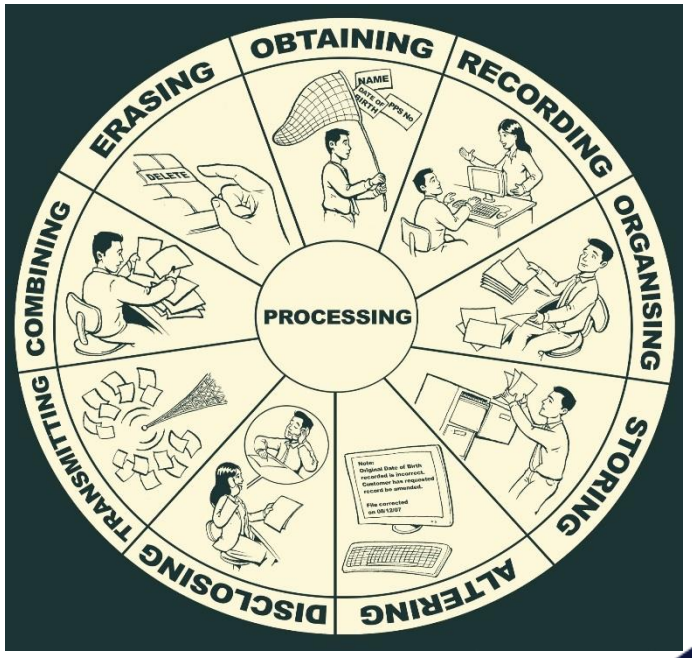
Definition of Personal Data (Article 4.1)

Identifiable Natural Person:

- Identified by an identifier such as a name, an identification number, location data or an online identifier
- Identified by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Definition of Processing (Article 4.2)

- Collecting
- Recording
- Organising
- Structuring
- Storing
- Adapting
- Altering
- Retrieving
- Consulting
- Using
- Disclosing
- Disseminating
- Aligning or combining
- Restricting
- Erasing
- Destroying



Definition of Data Controller (Article 4.7)

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

What does all of this mean?

If you're any kind of a business operation or public body, that does almost anything imaginable, to information relating to an identifiable person, for whatever purpose, in whatever way, the GDPR applies to you!!

Fair Processing

Essentials:

- ✓ consent of data subject

<u>or</u>

- ✓ other legitimate basis e.g. statute, contract, legitimate interest

<u>And</u>

- ✓ Processing must be proportionate and fair

Enhanced rights for individuals

- Subject Access Rights – no fee – 30 days to comply
- Right to Rectification and “Right to be Forgotten”
- Right to Restriction
- Right to Data Portability
- Liability and Compensation
- Administrative fines

Administrative Fines

- Article 83
- Up to €20m or
- 4% of global turnover for the preceding financial year

Enhanced Data Controller/Processor Obligations (Articles 24 to 43)

- Mandatory Breach Reporting (unless unlikely to result in risk)
- Security of Processing (risk based)
- Data Protection Impact Assessments (DPIA)
- Prior consultation with Supervising Authority (mitigation)
- Data Protection Officer
- New Consent Obligations

Mandatory Breach Reporting

Make sure you have the procedures in place to detect, report and investigate a data breach.

Top 5 Breach Report Categories 2016

1. Unauthorised Disclosures
2. Postal Disclosures
3. Electronic Disclosures
4. Website Security
5. Other Security Related Issues

Top 5 Complaint Types 2016

1. Access Rights (56%)
2. Disclosure
3. Electronic Direct Marketing
4. Unfair Processing
5. Failure to secure data

Article 29 (Directive 95/46/EC)

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as "the Working Party", is hereby set up. It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Current Article 29 Guidance

- Data Portability
- Data Protection Impact Assessment
- Data Protection Officer
- Establishing Lead Supervisory Authority

Future Article 29 Guidance

- Certification
- Profiling
- Consent
- Breach Notifications

Consent under GDPR (Article 4 “Definitions”)

’Consent’ of the data subject means any freely given specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Data Protection Officer (Articles 37, 38 & 39)

- Public Authorities
- Core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- Processing on a large scale of special categories of data (Articles 9 and 10)

Accountability

- Make an inventory of all personal data you hold
- Why do you hold it?
- Do you still need it?
- Is it safe?

Transparency

Tell individuals how you will use their data

Transparency

Policies & documented procedures in place to cover all areas

- General
- Data Retention
- Data Security
- Dealing with Access and other Requests
- Monitoring
- CCTV
- Direct Marketing
- Payment Processing
- Cookies
- Website Privacy

Dealing with Access Requests (Article 15)

Engage with data subject

Seek extension of time if necessary

Try to define scope

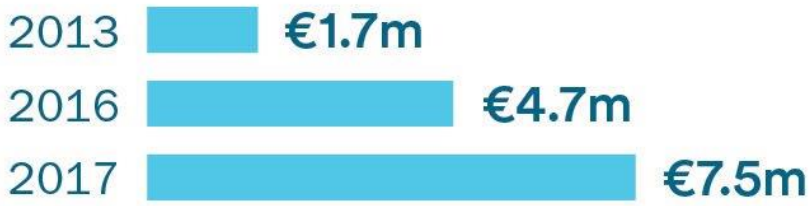
Limit expectations early

Explain exemptions applied

Data Protection Commissioner Role

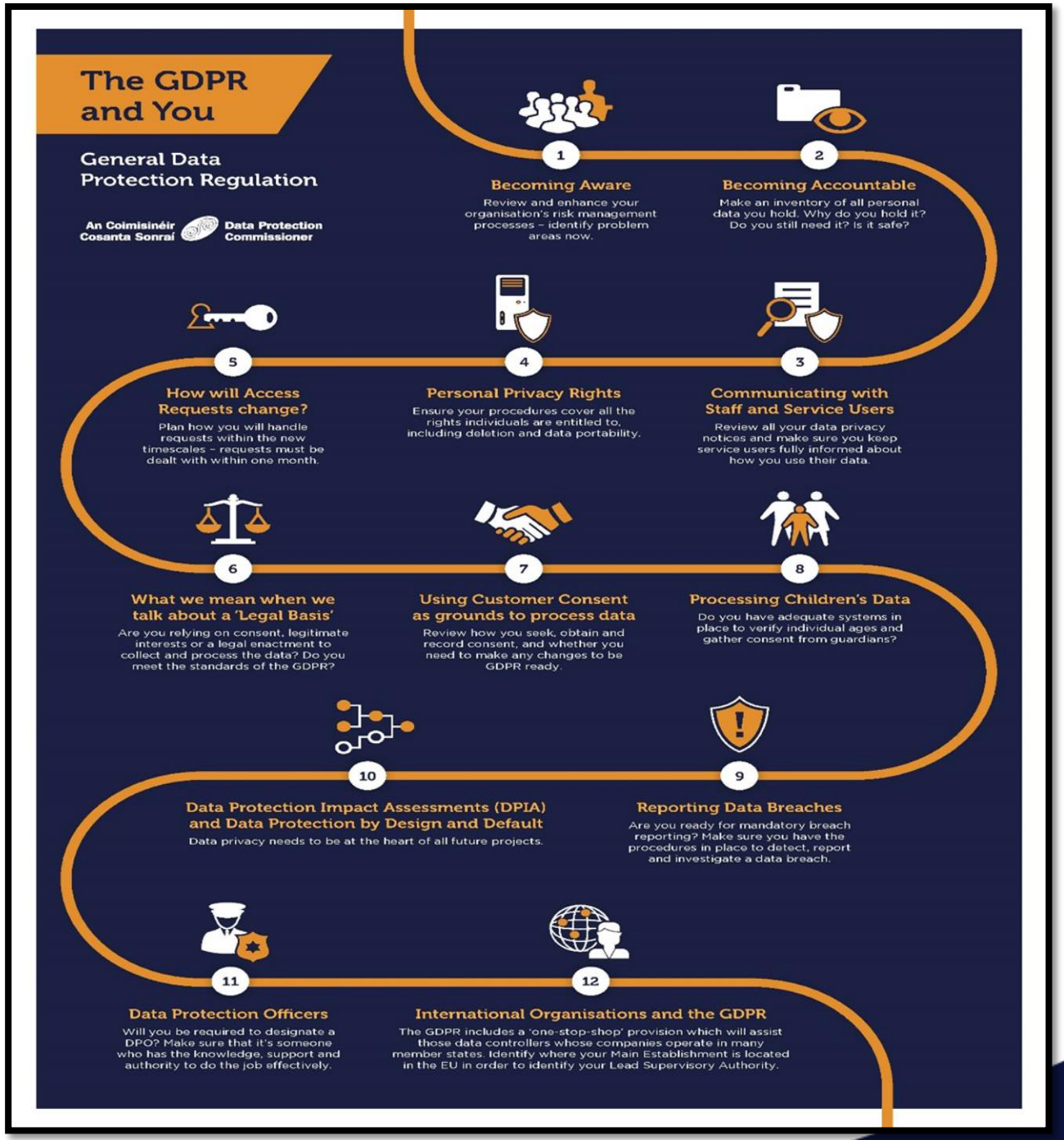
A Resourced and Effective Regulator

Funding



Staff

DPC Annual Report 2016



Brightwater TakeControl

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

Brightwater TakeControl

www.dataprotection.ie

@DPCIreland

info@dataprotection.ie

Thank You