GDPR OVERVIEW
The Journey So Far
22 July, 2020
Webinar starts at 11.00am
Todays Speakers

Ricky Kelly
Partner | Cyber and Data Protection

Aoife O’Sullivan
Solicitor | Cyber and Data Protection
Topics

- Data Protection Principles
- Refresher and key changes
- Lawfulness of processing & Transparency
- Records & Accountability
- Retention of Records
- Transfers
- Data Protection Relationships and Agreements
- Direct Marketing
- Rights of Data Subjects
- Data Security & Breaches
Personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimisation principle")
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures (the "integrity and confidentiality principle")
- The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle").
GDPR and Data Protection Acts - Existing law

What was repealed?


General Data Protection Regulation ("GDPR")

What has come into force?

- GDPR - Friday 25 May 2018

When did it happen?

- Data Protection Act 2018 (commenced on 24/25 May 2018)
GDPR at a glance

• **Stricter consent rules:** freely given, specific, informed and delivered by means of an unambiguous indication (Article 7)

• **Privacy by design:** privacy measures to be incorporated at product design stage (Article 25)

• ‘**One Stop Shop’:** multinationals predominantly regulated by a single supervisory authority (Article 56)

• **Data protection officers:** Some organisations are obliged to appoint DPOs (Article 37-39)

• **New rules on data notifications:** New rules on data breaches: without undue delay but no later than 72 hours

• **Stricter fines:** up to 4% of global turnover or €20,000,000, whichever is higher (Article 83). Section 141(4) DPA 2018- Public Authority not acting as an undertaking within the meaning of the competition Act- not more than 1,000,000

• **Right to compensation:** individuals are allowed to recover pecuniary as well as non-pecuniary damages (e.g. damages for distress) (Article 82)
Personal Data

Important to Remember:

1. Data Protection legislation only applies to Personal Data.
2. Does not apply to deceased individuals.
3. Information on companies/corporate entities – not personal data.
4. Anonymous data is not personal data.
5. Electronic and “relevant filing system”.

Personal data is defined in the GDPR as:

“any information relating to an identified or identifiable natural person”.

An identifiable natural person is defined as:

“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 Category Personal Data

Personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Person’s sex life or sexual orientation
“Processing”

- **Processing**
  
  “*any operation or set of operations which is performed on personal data* or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”
A “Data Controller”

A Data Controller means “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 …”

Essentially, a data controller is the entity that controls the:
1. purposes; and
2. means
of processing the personal data.
A “Data Processor”

Processor means “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.
Joint Controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
Lawfulness of Processing
In order to process personal data, Data Controllers must ensure that they have a **lawful basis** for doing so (Article 6).

**Consent**
The conditions for obtaining consent have become ** stricter** under the GDPR

**Definition in GDPR:**
“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”
Lawfulness of Processing - Consent

- Silence, inactivity or pre-ticked boxes will no longer be sufficient.

- Consent should not be “bundled” with other written agreements or declarations. It must be **clear** and **distinguishable**.

- Data subjects should be informed of their **right to withdraw consent** at any time. The method for withdrawing consent must be as simple as the method used for obtaining consent.

- **Separate consents** should be obtained for distinct processing operations.
Other Lawful Bases to process Personal Data

- **Performance** of a contract
- Compliance with a *legal obligation*
- Protect the vital interests
- The *public* interest
- **Legitimate interests** – provided such interests are not overridden by the interests and fundamental rights of the data subjects
Lawfulness of Processing – Article 9

• In order to process Special Category Personal data, data controllers must have a lawful basis under Article 6 and Article 9

• explicit consent

• obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

• vital interests

• necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
Lawfulness of Processing – Article 9

**Lawfulness of Processing - Article 9 & Section 50 of the Data Protection Act 2018**

Article 9(4) GDPR outlines that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

**Section 50 DPA 2018:**
Subject to *suitable and specific measures* being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of data concerning health shall be lawful where the processing is necessary and proportionate for the purposes of the following:

a) a policy of insurance or life assurance,
b) a policy of health insurance or health-related insurance,
c) an occupational pension, a retirement annuity contract or any other pension arrangement, or
d) the mortgaging of property.
Retention of Records
Retention of Records

Article 5(1)(e) GDPR:

- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with Art.89(1) and subject to the implementation of appropriate safeguards.

Three point test

- Records must be retained in accordance with the relevant statute
- Records should be retained if the controller requires or may require the records for the defence of legal proceedings
- Records may be retained in excess of the statutory period if required for the purpose for which they were collected
Retention of Records

- **Wages** - *The National Minimum Wage Act 2000 (Section 22)*: 3 year retention period.

- **Employment of Minors** - *Protection of Young Persons (Employment) Act 1996 (Section 15)*: 3 year retention period.

- **Hours Worked** - *Organisation of Working Time Act 1997 (Section 25)*: 3 year retention period from the date of creation.

- **Collective Redundancies** - *Protection of Employment Acts 1977-2007 (Section 18)*: 3 year retention period from date of creation.


- **Tax Records** - 6 year retention period – *Companies Acts and Taxes Consolidation Act 1997*

- **Health and Safety Records** - *The Safety, Health and Welfare at Work (General Applications) Regulations 1993 (Section 60)*: 10 year retention period from the date of the accident or dangerous occurrence.

- **Contracts of Employment** - *Terms of Employment (Information) Act 1994*: requires that an employee’s terms and conditions of employment be retained for the duration of the employment. *Statute of Limitations 1957 - 6 years from the termination of the employment.*

- **Personal Injuries** - 2 years from date of cause of action and a period of 3 years is the general recommended retention period.
International Data Transfers
International Data Transfers
General Rules

• **General Rule:** Transfers of personal data to third countries (outside of the EEA) are prohibited, unless the country ensures an adequate level of protection to personal data.

• “Transfer” is interpreted broadly to mean not only moving the data but also accessing from a location outside of the EEA, storing on a server located outside of the EEA, storing in a cloud controlled by an entity established outside of the EEA.
• **Adequacy decisions** - Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and Japan as providing adequate protection.

• **Appropriate safeguards:**
  • **Binding corporate rules** – officially recognized. Previously, some authorities insisted on approving specific data transfers even after the binding corporate rules had been approved.
  • **Model Clauses** – controller to controller and controller to processor.
  • **Privacy Shield** – Self-certification framework which imposes obligations on companies handling personal data and contains safeguards and transparency obligations in relation to US government access.
  • **New mechanisms** – derogations for specific situations.
The DPC has issued guidance on transfer of personal data from Ireland to the UK in the event of “deal/no-deal” Brexit.

What types of processing activities and organisations might be impacted:

- outsource their HR, IT and Payroll functions,
- use UK based marketing services providers to send marketing communications,
- use occupational health providers based in the UK,
- use pensions providers based in the UK,
- storing Data in the UK on a server or the cloud.
DPC - Guidance Re “Deal/No-Deal” Brexit

• **DEAL**: If there is a negotiated deal to regulate the UK’s relationship at the end of the transition period, then the exact effects on data transfers will depend on the nature of that deal.

• **No DEAL**: UK to move outside the EU/EES and become third Country for the purpose of GDPR similar to Australia and India.

• EU organisations will not permitted to transfer personal data to UK organisations unless certain standards are in place and maintained.

• What must be put in place?

  - specific safeguards to protect the date in the context of its transfer and subsequent processing i.e. Standard Contract Clauses
Data Protection Relationships
Refresher – Data Flows

Data Flows Diagram:
- Data Controller
- Personal Data
- Data Subjects
- Data Processor

Data Flows:
- Data Controller to Data Subjects: Personal Data
- Data Subjects to Data Controller: Personal Data
- Data Controller to Data Processor: Personal Data
- Data Processor to Data Controller: Personal Data
Controller / Processor relationship

Article 28(1)
“Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

Article 28(3)
Appointment - a binding written agreement which sets out a number of conditions that must be met by the Supplier/Processor.
Article 28(3)- Mandatory provisions of Data Processing Contracts

- Documented instructions from the controller.
- Commit to confidentiality
- Take all security measures as prescribed by article 32 [security of processing]
- Abide by the rules for engaging a sub-processor
- Implement toms to assist controller in complying with rights of data subjects
- Assist controller with security requirements, breach notifications and DPIA
- Delete or return personal data to the controller
- Demonstrate compliance with the above (through audits and inspections)
Other provisions which may be included in data processing contracts

- Other provisions may include but are not limited to:
  1. Liability provisions (including indemnities);
  2. Detailed (technical) security provisions; and/or
  3. Additional cooperation provisions between the Controller and Processor.
  4. International transfer of personal data
Controller / Controller relationship

- **No legal obligation** under the GDPR or the Data Protection Act 2018 to put in place an agreement between individual data controllers who process/share personal data.

- **Good practice** to put data sharing agreements in place:
  1. Demonstrate compliance with GDPR (Article 5 GDPR)
  2. Ensure that each party is aware of its responsibilities & Obligations under GDPR.
Joint Controllers-
Article 26

• shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them..............

• The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
Direct Marketing and the impact of the GDPR regarding consent
Direct Marketing

- The DPC describes Direct Marketing as **involving a person being targeted as an individual, and the marketer attempting to promote a product or service, or attempting to get the person to request additional information about a product or service.**

- Unaddressed mail received at your home is not covered by data protection legislation as no personal data is used.

- Direct marketing covers **all advertising or promotional material**, including promoting the aims or ideals of not-for-profit organisations-for example, it covers a charity or political party campaigning for support or funds.
Direct Marketing

Current Legal Framework

• The Irish Data Protection Acts 1988 to 2018
• the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")
• the ePrivacy Directive (which was implemented into Irish law by the ePrivacy Regulations)
• DRAFT ePrivacy Regulation
• General rule for electronic direct marketing is that it requires clear affirmative consent of the recipient (such as by specifically opting-in) under Regulation 13 of the ePrivacy Regulations (SI 336/2011).

• This consent must be GDPR consent (Article 7 of GDPR)

• Silence, inactivity or pre-ticked boxes will no longer be sufficient.

• Consent should not be “bundled” with other written agreements or declarations. It must be clear and distinguishable.

• Data subjects should be informed of their right to withdraw consent at any time. The method for withdrawing consent must be as simple as the method used for obtaining consent.

• Separate consents should be obtained for distinct processing operations.
Exception to obtaining consent in relation to existing customers (Soft opt in)

- The product or service being marketed is Laya’s own product or service;
- The product or service Laya is marketing is of a kind similar to that which you sold to the customer at the time you obtained their contact details;
- At the time you collected the details, you gave the customer the opportunity to object, in an easy manner and without charge, to their use for marketing purposes;
- Each time you send a marketing message, you give the customer the right to object to receipt of further messages; and
- The sale of the product or service occurred not more than twelve months prior to the sending of the electronic marketing communication or, where applicable, the contact details were used for the sending of an electronic marketing communication in that twelve-month period.
Article 21(2) GDPR

- Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

- Where an individual objects to processing for direct marketing purposes, the personal data must no longer be processed for those purposes. The DPC advise organisations to keep a “do not email or text list” (also known as a suppression list) of those who object of opt out of direct marketing.
Since May 2018, the DPC has opened approximately 282 new direct marketing complaints and concluded approximately 247. A total of 85 of those new complaints were opened in the first five months of 2020 and 78 complaints have been concluded this year to date.

In the course of its investigations into these matters the DPC also identifies potential GDPR-related systemic issues that will result in the DPC instigating separate inquiries under the GDPR and the Data Protection Act 2018.
Different rules depending on the type of direct marketing

<table>
<thead>
<tr>
<th>Type of individual</th>
<th>Text/Email marketing</th>
<th>Phone Marketing to land lines</th>
<th>Phone marketing to Mobile phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Customer</td>
<td>Opt out (provided you are marketing a similar product or service and other conditions, as outlined above are met).</td>
<td>Opt out (unless they have notified you directly or by notifying the National Directory Database (NDD)). All marketing messages sent by this communication must include the identity of your organisation as the caller and a contact address or Freephone number for opt-out.</td>
<td>Opt out (unless they have notified you directly or by notifying the National Directory Database (NDD)).</td>
</tr>
<tr>
<td>Individual Non Customer</td>
<td>Opt in If an individual is not a customer, you may not use email to send unsolicited direct marketing material to them unless you have obtained the prior consent of that individual to receive such messages.</td>
<td>Opt in All marketing messages sent by this communication must include the identity of your organisation as the caller and a contact address or Freephone number for opt-out.</td>
<td>Opt in</td>
</tr>
<tr>
<td>Business contacts Customer &amp; Non Customer</td>
<td>Opt out – it is best practice to wherever possible obtain a full opt in rather than relying on opt outs as a long term strategy.</td>
<td>Opt in if on National Directory Database (NDD), Opt out otherwise. All marketing messages sent by this communication must include the identity of your organisation as the caller and a contact address or Freephone number for opt-out.</td>
<td>Opt in</td>
</tr>
</tbody>
</table>
Rights of Data Subjects
1. Data subjects have the right to obtain certain information from Data Controllers

2. DSAR exemptions under GDPR and Data Protection Act 2018
Subject Access Requests

Time limits for complying with the rights of data subjects

• Article 12(3) to 12(4)
  • A controller must, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of data subjects.
  • If the controller fails to meet this deadline, the data subject may complain to the relevant DPA and may seek a judicial remedy.
  • Where a controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.
Further Data Subject Rights

- The GDPR enshrines a wide range of existing rights under the DPA and also introduces new rights for individuals in respect of their personal data.
  - **Right to rectification**: the right to correct any inaccurate personal data.
  - **(Enhanced) right to erasure**: the ‘right to be forgotten’ allows for the right to the removal of data.
  - **Right to restrict processing**: the right to restrict certain processing of personal data – replaces ‘blocking’ in dpa.
  - **(New) right of data portability**: the right to request the porting of one’s data to a new service provider.
  - **(Updated) right to object**: the right to object to certain processing activities of the data controller.
  - **(Enhanced) automated decisions**: rights in relation to decisions made by automated processes which significantly affect them (inc. Profiling).

- Perfect storm of requests?
Data Security and Data Breaches
What is a Cyber Security Incident?

Cyber Security Incident - an incident that results in unauthorised access to data, applications, services, network and/or devices by bypassing their underlying security mechanisms.

- Cyber Security Breaches will almost always require an investigation into potential data breaches.
- Security breaches can be attributed to a hacking or malware attacks but can include:
  - Insider leak
  - Payment card fraud
  - Loss or theft
  - Unintended disclosure
  - Unknown
What is a Personal Data Breach?

Articles 4(12) of GDPR

“Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed”

Article 32 (1) of GDPR – Security of Processing

• Organisations are required to take steps to ensure the security of it processing. This includes the implementation of Technical and Organisations Measures to ensure a level of security appropriate to the risk.

• What to consider when determining the appropriate measures:-
  • The state of the art;
  • The cost of implementation; and,
  • The nature, scope, context and purpose of the processing.
Examples of Security Threats

1. Insider threats
2. Online Identity Theft
3. Malware
4. Mobile Phone, Laptop and mobile device theft
5. Website Defacement
6. Cardholder Data Compromise
Why important
Damage to Reputation

• The effect of a data breach can come in the form of damage to reputation due to a perceived betrayal of trust and fear of financial losses should such records be compromised.

• A study into consumer behaviour in the aftermath of a Data Breach has shown that up to a third of customers in the retail, finance and healthcare sectors will stop doing business with an organisation that has reported a breach.

• Underarmor App – MyFitnessPal – Reported Data Breach on Thursday, 28 March 2018. Share loss of 10% since notification and continue to deal with the breach.
Theft and Extortion may extend to:
- Financial information/data,
- Customer, supplier or client data,
- Employee data,
- Trade Secrets and Intellectual Property,
- Network configurations and/or cyber security setting.

Theft can be a simple copying process or result in the destruction by encryption or otherwise of the original source data.

Trend Micro predicted that ransomware would continue to be a cybercrime mainstay throughout 2018, while other forms of digital extortion would gain ground.
Why important
Loss of Operations

Loss of access to necessary network systems (DDoS) or otherwise.

Consequences can be very significant in terms:

1. IoT devices – cameras, routers etc.
2. Loss of revenue;
3. Loss of trust; and,
4. Diversion of Management time.

Trend Micro predicted that losses from Business Email Compromise Scams would exceed $9 billion in 2018.
Threats may come from, amongst others:-

- **Data Subject claims** for material and non-material loss;

- **Joint Liability** for Controller and Processor (Article 82(4) of GDPR provides that each party shall be held liable for the entire damage in order to ensure effective compensation of the data subjects);

- **Breach of Contract**;

- **Data Protection Investigations** (Investigations from Regulators (Independent News Media)).
Article 33 of the GDPR and Section 86 of the Data Protection Act 2018 provide as follows:

“In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay”.
Article 34 (1) of the GDPR and Section 87 of the Data Protection Act 2018 provide as follows:

“When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.”
Controller Notifications Obligations

- Categories of Data Breaches:
  - Confidentiality Breach
  - Integrity Breach
  - Availability Breach
- Without Delay and where feasible not later that 72 hours
- When will an organisation be deeded to have become aware?
  - Technical and Organisations Measures
  - Initial investigation stage
Controller Notifications Obligations

- **Determining likelihood of Risk**
  - Assess the Risk i.e. physical, material or non-material damage for individuals whose data is the subject of the breach.
  - Factors to be considered – Likelihood/Severity
    - The type of breach
    - The nature, sensitivity, and volume of personal data
    - Identification of Individuals
    - Severity of Consequences for Individuals
    - Special characteristics of the individual and Data Controller
    - The number of affected individuals
Controller - Notifications Obligations

• Guidance from the DPC on Risk

**Should take into account:**

- The cause of the breach
- The types of data exposed
- Mitigating factors (i.e. encryption)
- Whether data relating a child or other persons who, by reasons of their physical or mental incapacity, are unable to act on their own behalf.

**Level of Risk:**

- Low
- Medium
- High
- Severe
Data Security Incident Response
Data Security Incident Response

**PHASE 1**

Respond

- **Step. 1** Identification and Initial Assessment
- **Step. 2** Containment and Recovery
- **Step. 3** Risk Assessment
- **Step. 4** Notification
Data Security Incident Response

Step. 1: Investigate & Prepare Report
Step. 2: Manage Third Party Investigations
Step. 3: Reputation Management
Step. 4: Evaluation and Response

PHASE 2
Follow Up
GDPR
2 years on
Life After 25 May 2018 – Statistics

• **Total cases opened** – 15,025 (largest percentage relate to DSARs)

• **12,437 data security breaches** recorded (unauthorised disclosure represents 80%)

• **77 statutory inquiries** – 24 cross-border and 25 national.

• **First fine issued for €75,000** to State Agency

• The DPC received 1,823 new **Data Protection Officer notifications**

• **282 direct marketing complaints**
Questions?

Read more of what we’re discussing at www.rdj.ie