idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

GDPR

General Data Protection Regulation

Its application for Businesses

David Cauchi
Head Compliance

Regulation (EU) 2016/679

…on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

NO REVOLUTION

but

an EVOLUTION of the existing framework

How does personal data affect you and your business?

What is your role?

Data Controller

"…a person who alone or jointly with others ***determines the means and purposes*** *of the processing of personal data"*

Who is the Data Controller?

In the case of Business Organisations normally the Data Controller is the Head of Organisation or Managing Director

Processor

"…a person who processes personal data on behalf of a controller"

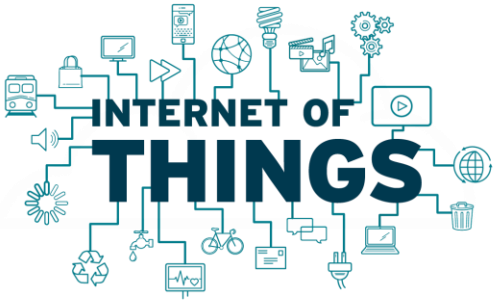
Who can be a processor?

Any person or entity engaged by the data controller to provide a particular service and entrusted with the processing of personal data necessary to render such service.

Examples: Provision of IT services, Accountancy.

Technology and global players radically changed the way personal data is processed

Google™



Microsoft Cloud

skype™

Need for change

- Information is becoming increasingly exposed and vulnerable leading to security breaches, hacking or other unlawful action especially in the globalised online environment.
- Data protection and privacy challenges are on the increase.
- Modernising the existing set of data protection rules was part of the EC's Digital Single Market strategy.
- More accountability, consistency and harmonisation across the EU.
- Rebalancing of rights in a digital world.
- Provide legal certainty for economic operators.

Main principles and elements underpinning the GDPR

Accountability Principle

Ability to demonstrate compliance.

Empowerment to the user

User controls through a privacy dashboard.

Granular options.

Scalable and transparent.

Privacy by default settings.

Proximity Principle

In cases of cross border breaches, the data subject may complain to the national DPA.

One-Stop-Shop

Consistency mechanism.

Shift from *ex-ante* to *ex-post*

Generally, no notification to the DPA.

Powers of the Commissioner

Investigative powers

- access personal data being processed;
- obtain information on the processing of personal data and its security;
- enter and search any premises with the same powers as are vested in the executive police;

Corrective powers

- issue warnings and reprimands to the controller and processor;
- order rectification or erasure of personal data;
- impose temporary or definitive ban on the processing activity;
- impose administrative fines [a.83 of the GDPR – effective, proportionate and dissuasive – up to a maximum of 4% of annual turnover or €20 Million].

Powers of the Commissioner

Authorisation and advisory powers

- authorise processing which is subject to a prior checking requirement;
- issue opinions and approve draft codes of conduct;
- advise the Parliament, Government and the general public on any issue related to the protection of personal data;
- accredit certification bodies.

Engage in legal proceedings

- any person aggrieved by a decision of the Commissioner may appeal to the Data Protection Appeals Tribunal;
- recourse to the Court of Appeal shall also lie to a party or to the Commissioner where they feel aggrieved from a decision of the Tribunal;
- Commissioner may institute proceedings in a Court of law against any person.

Scope

- Material Scope:

  - **applies to the processing of personal data.**

- Territorial Scope:

  - **applies to data controllers and data processors with an establishment in the EU; or**

  - **having an establishment outside the EU that targets individuals in the EU by offering goods and services.**

  In similar cases, a representative established in an EU MS shall be appointed.

Conditions for consent

freely-given, specific, informed and unambiguous indication of the data subject's wishes given by a statement or by a clear affirmative action

- Data controller shall be able to demonstrate that the data subject has consented to the processing of data.
- Consent shall be presented in a manner which is clearly distinguishable from other matters.
- Use of clear and plain language in the information clauses.
- Silence, pre-ticked boxes or inactivity should not therefore constitute consent (Recital 32).
- The right to withdraw consent (easy to withdraw as to give consent).

Conditions for consent

- Explicit consent is required:

  - in certain situations of serious data protection risks
  - where a high level of individual control is deemed appropriate.

- Explicit consent applies in the following cases:

  - processing of special categories of data (A.9)
  - data transfers to third countries in the absence of adequate safeguards (A.49)
  - automated individual decision making (profiling) (A.22).

- Shall be obtained in a clearly separate fashion.

- Ideally, in a written statement to remove doubt and potential lack of evidence.

Other legal criteria

- Consent is not the only option for processing.
- Other possible criteria:
  - ✓ Performance of a contract
  - ✓ Legal obligation
  - ✓ Vital interest
  - ✓ Public interest
  - ✓ Legitimate overriding interest
- Organisations should carefully consider which legal criteria is appropriate for their processing operations.
- More stringent criteria apply for special categories of data.

Direct Marketing

- In case of marketing communications sent out by conventional mail / post or made by telephone, the **OPT-OUT** regime applies.
- Recital 45 of GDPR recognises that the processing for direct marketing may be regarded as in the legitimate interest.
- Data subject has the right to object
  - ✓ at any time
  - ✓ free of charge;
- This right should be explicitly brought to the attention of the individual.

Direct Marketing

- In cases where the marketing communication is sent out by email, fax or SMS, the **OPT-IN** regime applies.

- **prior consent in writing**

  Exception **(SOFT OPT-IN)**

- Where the contact details are obtained in the context of a sale and provided that they are used by the same company to market s**imilar products or services**.

- Opt-out must be offered upon obtaining the information and with each message sent.

Information to data subjects

- Transparency principle (A. 5(1)(a))
- Provided at the time the personal data are collected from the data subject (A.13)
- Information to include:
  - purposes of processing
  - the intention to transfer personal data to a third country
  - retention period or criteria used to determine that period
  - the existence of data protection rights
  - the right to withdraw consent
  - the right to lodge a complaint with the DPA
  - the existence of automated decision making.

Information to data subjects

- Using clear and plain language
- Easily accessible
- Use of layered notices to avoid information fatigue:
  - information is not provided in a single notice
  - allowing users to navigate through the section they wish to read
  - first layer should provide a clear overview of the information *(information which has the most impact on the data subject)*
  - clear indication where to find additional information
- Incorporating in the architecture a privacy dashboard – a single point where to view privacy information and manage preferences.

Retention of records

- General requirement (A.5(1)(e))

"Personal data shall be kept in a form which permits identification of data subjects for ***no longer than is necessary*** *for the purposes for the personal data are processed"*

Right of access

Data controller shall provide , **within one month**, **a copy** of the personal data undergoing processing together with access to other information:

- purpose of processing
- categories of personal data concerned
- recipients to whom the personal data have been disclosed
- where possible, the envisaged retention period
- the existence of the rights to rectify, erase or restrict processing
- the right to lodge a complaint with the DPA
- the existence of automated decision-making, including profiling, and other meaningful information about the logic involved and envisaged consequences.

Right to data portability

- The right to receive personal data which the data subject has provided to the controller:

  - **in a structured, commonly used and machine-readable format**.

- Applies where processing is based on consent or a contract and by automated means.

- Transmitted to the data subject or directly to another data controller without hindrance from the original controller and where technically feasible.

- Underlying scope is to allow individuals in quickly changing from one service provider to another, without unnecessary obstacles due to their data.

Role of Processor

- GDPR strengthens the current obligations by introducing more prescriptive rules on processors:

  - Controllers shall only use processors providing sufficient guarantees to comply with the GDPR;

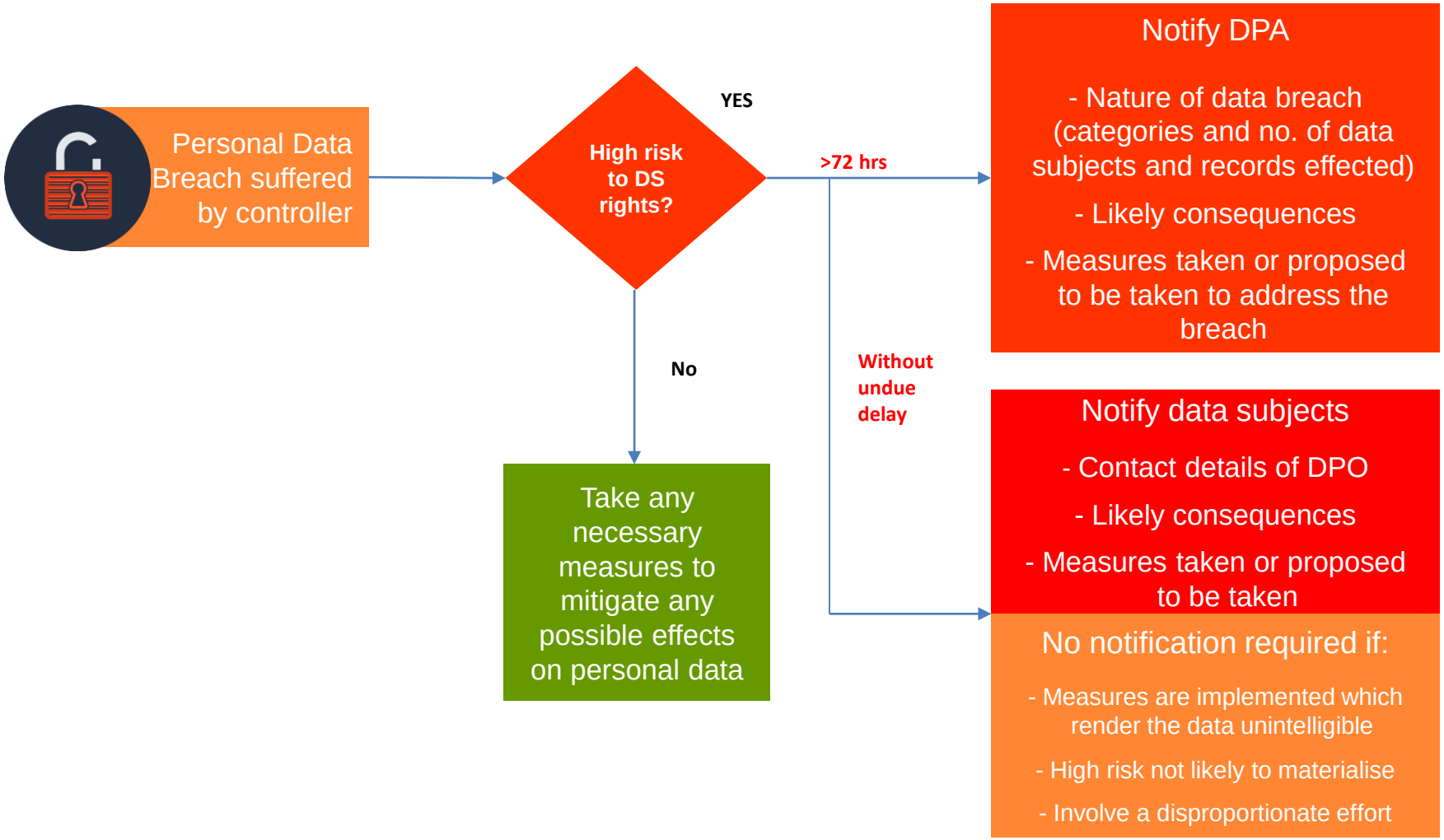
  - Sub-processing only allowed with prior written authorisation from data controller;

  - Processing shall be regulated by means of a binding contract in line with the terms provided under A.28;

  - Standard contractual clauses may be developed by COM or MS DPAs.

- GDPR extends responsibilities of data controllers on processors for certain obligations

Notification of personal data breach



Security of processing

- Data controller shall implement adequate organisational and technical measures to ensure a level of security appropriate to the risk including:
  - pseudonymisation and encryption of data
  - ability to ensure ongoing integrity and resilience of processing systems
  - ability to restore the availability of processing systems in a timely manner in the event of an incident
  - the regular testing, assessing and evaluating the effectiveness of security measures.

- To demonstrate compliance with the security requirements, the controller may adhere to:
  - an approved code of conduct (prepared by associations or bodies representing the sector)
  - an approved certification mechanism.

Data Protection by design and default

- Considerations should be made at an early stage and throughout the lifecycle (e.g. developing IT systems, introducing legislation or measures affecting privacy).
- Data protection embedded in the design.
- Proactive and preventive privacy-friendly measures (e.g. pseudonymisation, data minimisation).
- Default measures tailored to automatically protect individual's privacy (e.g. preset storage periods, limited data collection and accessibility, user-friendly options).

Data Protection Impact Assessment

- Required to be carried out by the controller in the following cases:

  - processing operation is likely to result in high risk;

  - systematic and extensive evaluation of data subjects based on automated processing (including profiling);

  - processing of special categories of personal data on a large scale.

- Prior consultation with DPA required if the Data Protection Impact Assessment indicates that processing involves a high risk to data subjects.

Records of processing activities

- GDPR introduces new requirement to keep a record of processing activities:
  - applicable to both controllers and processors
  - substitutes the notification currently submitted to the DPA.
- The new obligation applies:
  - for organisations employing 250 persons or more
  - when processing involves special categories of data
  - when processing likely to involve risks for data subjects.
- Records of processing activities shall be made available to the DPA upon request.

Data Protection Officer

- Mandatory designation in the following cases:

  - processing carried out by public authorities/bodies

  - regular and systematic monitoring of data subjects on a large scale

  - processing of special categories of data on a large scale.

- A single DPO may be appointed to serve for a group of undertakings or public authorities/ bodies.

- GDPR requires DPO to have expert knowledge of data protection law.

Data Protection Officer

- Position and Tasks of DPO:

  - staff member or engaged on service contract
  - should be able to work independently
  - involvement in data protection matters
  - informing and advising controller/ processor;
  - monitoring compliance;
  - providing advice and monitoring DP Impact Assessment;
  - cooperate with the DPA;
  - act as contact point for data subjects and DPAs.

- Controller or processor shall publish contact details of DPO and communicate them to DPA.

Final remarks

- Take stock of the current processes involving personal data and conduct an internal audit to identify any compliance gaps.
- Review the internal structure of the organisations and introduce the necessary changes as required.
- Get your business priorities right!
- Legal duty of the data controller to observe compliance with the GDPR.
- Interpretative guidance material is being and will continue to be issued by the WP29 and future EDPB.
- IDPC assists whenever requested and when necessary.

More rights for your personal data !

1 Data to take away !

I can get back the data I provided to an organisation or online-service and transmit those to other ones (social networks, Internet service provider, online streaming supplier, etc.)

2 Better transparency

I know what is done with my data and it's easier for me to exercice my rights.

3 Child protection

Online services must obtain the parents' consent before registering any child under 16 or less if provided by national laws.

4 One-stop-shop

In case of problems with how my data is handled, I can contact my national data protection authority, whatever the country where the organisation is processing my data.

5 Bigger sanctions

When infringing the regulation, the organisation at fault can be fined up to 20 000 000 € or 4% of its annual worlwide turnover.

Illustration : Marin Vidberg

6 Right to be forgotten

I can ask search engines to delist a web page that affects my privacy negatively or ask a website to erase an information, under certain circumstances.

The European data protection regulation

After 4 years of discussions at the European Union level, a final draft of the data protection regulation has been released. It is expected to help Europe face the challenges of the digital age. The regulation will strengthen the citizens' rights and provide them with real control over their personal data. It will offer an unified framework for companies and simplify the prior notification. The regulation will be formally ratified in early 2016 and will come into force in 2018 in all the Eu countires.

ARTICLE 29
Data Protection Working Party


KEEP
CALM
AND
PREPARE FOR
GDPR


THANK YOU