idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

GDPR

General Data Protection Regulation

Ian DEGUARA - Director
Office of the Information and Data Protection Commissioner

Regulation (EU) 2016/679

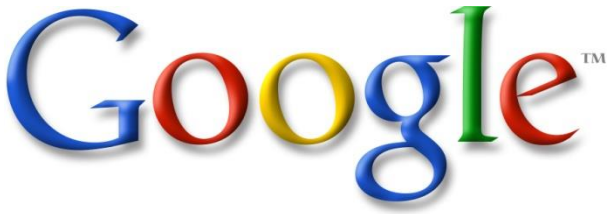
…on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

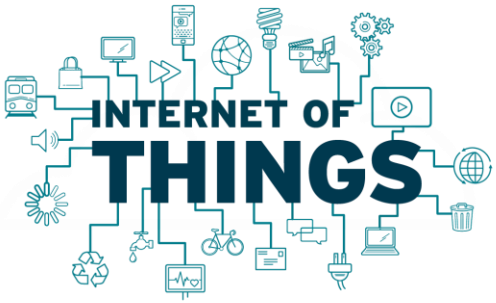
NO REVOLUTION

but

an EVOLUTION of the existing framework

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

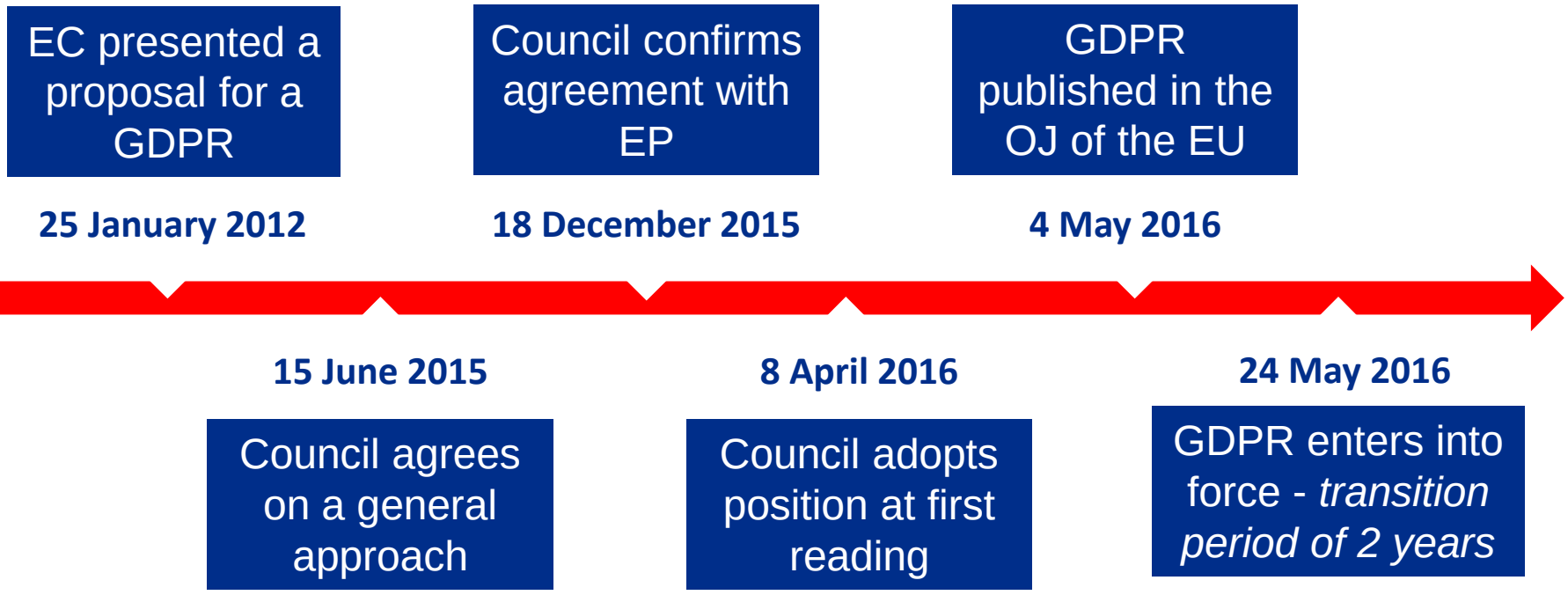




Need for change

- 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.

Timeline


EC presented a proposal for a GDPR
25 January 2012
15 June 2015
Council agrees on a general approach
Council confirms agreement with EP
18 December 2015
8 April 2016
Council adopts position at first reading
GDPR published in the OJ of the EU
4 May 2016
24 May 2016
GDPR enters into force - transition period of 2 years

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 offers 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

- In principle, consent is not a valid legal ground in the employment context.
- Not freely-given due to imbalance of powers (recital 43):
  - dependency resulting from employer/employee relationship where the employee may experience fear or risk of detrimental effects as a result of a refusal.
- Exceptions may exist (e.g. filming activity at the workplace).
- Conditionality (A.7(4)):
  - not desirable (lack of choice) to tie the provision of a contract to a request for consent to process data that are not necessary for the performance of such contract.

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.

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

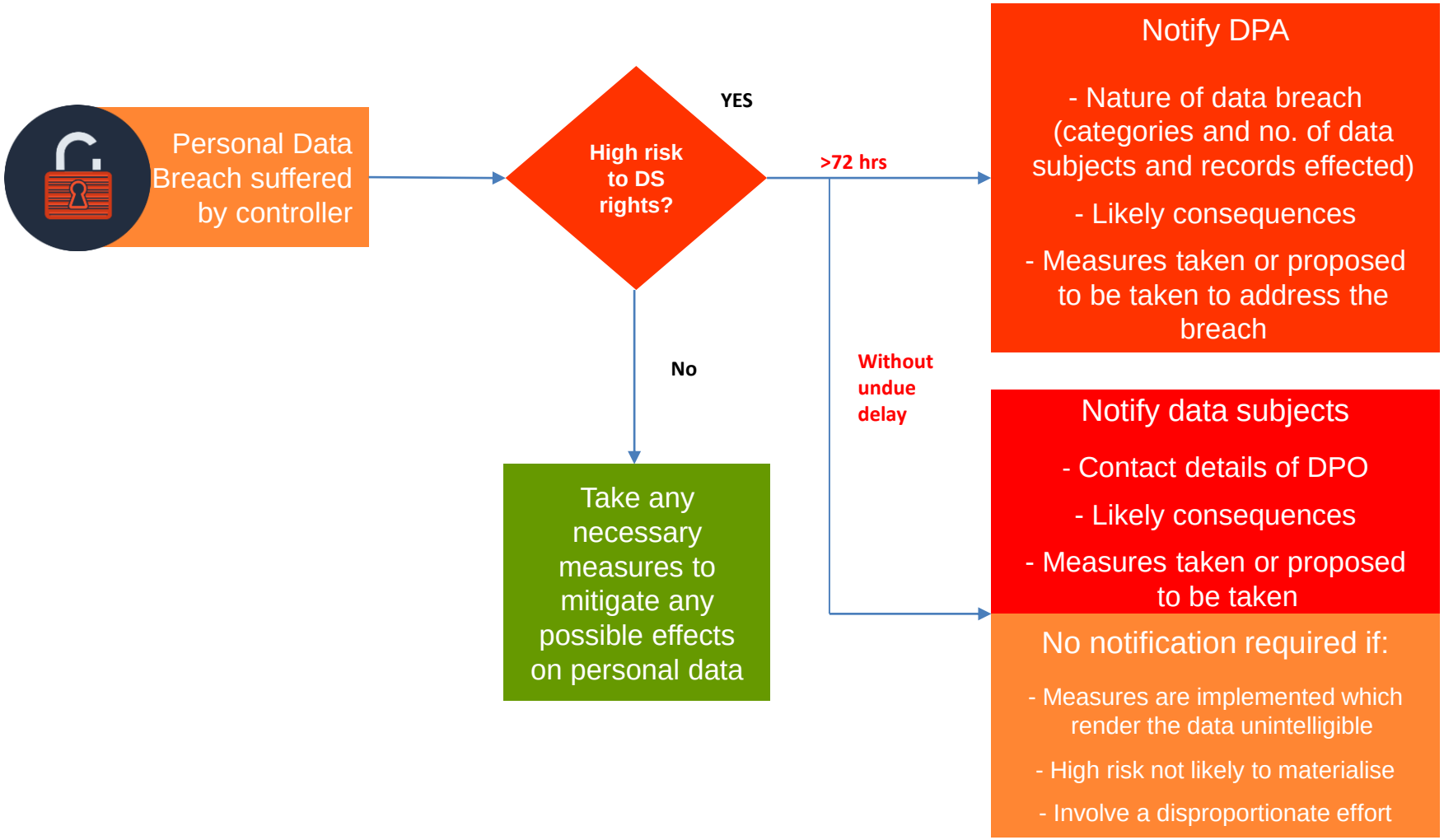
- The right to receive personal data which the data subject has provided to the controller:

  - **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.

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).

Certification

- Data protection certification mechanisms and data protection seals and marks which may used to demonstrate compliance with the GDPR;
- Voluntary and shall not diminish the compliance responsibilities of controllers and processors for compliance;
- Issued by the DPA or a certification body accredited by the DPA or by a national accreditation body;
- Certification is valid for a maximum of 3 years (maybe renewed) and issued on the basis of criteria approved by the competent supervisory authority;

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.

One-Stop-Shop

- A company with several subsidiaries in other MS may choose to deal with the DPA in the MS of its **main establishment** - "...*the place of its central administration in the Union...*".

- This principle intends to establish mechanisms to create consistency in the application of data protection across the EU.

- Co-decision making process is triggered in cross-border complaints:

  - Lead Supervisory Authority - cooperates with other concerned supervisory authorities for the purpose of exchanging the necessary information (Mutual assistance or Joint operations);

  - draft decision taken by the LSA

  - one or more concerned SAs expresses a **relevant and reasoned objection**

  - where the LSA decides not to follow such objection, it shall refer the case to the EDPB for a **binding opinion**.

Take-away messages

MESSAGE 1

Ensure to legitimise the processing on the strength of the proper legal basis.

MESSAGE 2

Consent obtained under the present legal framework shall continue to be valid to the extent that it is in line with the conditions of the GDPR.

MESSAGE 3

Consider appointing a Data Protection Officer even when not legally required.

Take-away messages

MESSAGE 4

Consider the capabilities of your systems to ensure, *inter alia*, their ability to:

- handle requests for access, portability, rectification, restriction and erasure
- safeguard the personal data
- detect data breaches
- facilitate the execution of certain requirements e.g. automated deletion.

MESSAGE 5

Ensure to accede to data subjects' rights in a proper and timely manner.

Take-away messages

MESSAGE 6

Develop policies to govern the processing of personal data, *inter alia*, concerning:

- Employee monitoring (email and internet access, vehicle tracking)
- CCTV cameras
- Recruitment process
- Other HR practices - access to employees' email following termination of employment

MESSAGE 7

Ensure that exiting contracts of employment and data protection policies and practices are GDPR compliant.

Take-away messages

MESSAGE 8

Observe the principle of storage limitation by determining retention timeframes:

- classify internal employment and other records
- assess legal, business and operational requirements
- develop retention policy
- be able to justify the storage periods.

MESSAGE 9

Any international transfer of employee data should take place only where an adequate level of protection is ensured.

Take-away messages

MESSAGE 10

Implement adequate organisational and technological security safeguards appropriate to the risk.

MESSAGE 11

Employers can rely on legitimate interest when conducting monitoring at the workplace. Lack of information, excessive and/or disproportionate processing constitutes an unjustifiable and intrusive activity.

MESSAGE 12

Conduct an internal audit to identify any gaps in the processes and address them accordingly.

Final remarks

- 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 in accordance with its work plan.
- OIDPC assists whenever requested and when necessary.

If you are not able to PROTECT
do not COLLECT