idpc.
INFORMATION AND DATA PROTECTION COMMISSIONER

General Data Protection Regulation (GDPR)

Saviour CACHIA - Commissioner
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.

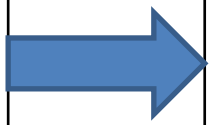
Current DP Legal Instruments

EU DP Legal Framework

- Directive 95/46 (DP Directive)
- Directive 2002/58 (e-Privacy Directive)
- Council Decisions (Police and Judicial co-operation)

Council of Europe

- Convention 108
- Rec. 87/15 Police Sector



National Law

- Data Protection Act (Cap. 440)
- S.L. 440.01 (Electronic Comms.)
- S.L. 440.06 (Police and Judicial co-operation)
- Other S.L.
- Ratified 28 Feb. 2003
- S.L. 440.05 Police

Reasons for Change

- Rapid technological developments
- Globalisation – increase in e-Commerce
- **Rebalancing of rights in a digital world**
- **More Accountability**
- **Stronger enforcement** for more effective protection
- **Consistency and harmonisation** across the EU
- Provide legal certainty for economic operators
- EU's Digital Agenda – rebalancing of rights

Future DP Legal Instruments

EU DP Reform Package

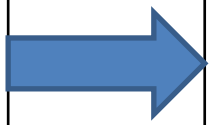
- General DP Regulation (Reg. EC 2016/679)

- Police Directive (EC 2016/680)

Supplemented by:

- e-Privacy Regulation

- CoE 108 Modernised



National Law

- General DP Regulation (Reg. EC 2016/679)

- DPA & S.L.

- S.L. Transposing Police Directive

Supplemented by:

-e-Privacy Regulation

- CoE 108 to be ratified

What is DP?

CREATING THE RIGHT BALANCE BETWEEN

Individuals / Clients

Business/Government Organisations

Employees

Employers

RIGHTS OF DATA SUBJECTS

NEED FOR DATA PROCESSING

Basic DP Compliance

- Identify legal basis
  - legal obligation, contract, legitimate interest

- Observe requirements for processing
  - purpose & storage limitation, safeguards, data minimisation

- Ensure data subjects rights
  - Information prior to processing (DP Policies)
  - Subject Access Requests – **copies of data**
  - Request for rectification or blocking or deletion

- Controller – Processor governed by a contract
  - Controller remains responsible
  - Liability clauses in case of data breaches

- Transborder data flows

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 More transparency

I know more about 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.

4 One-stop-shop

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

5 Bigger sanctions

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

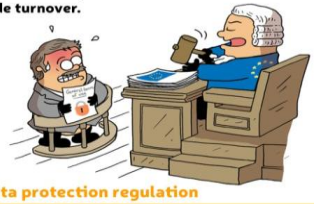


Illustration: Martin Vidberg

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

CNIL.

Data Retention Considerations

Legal obligations:

e.g. Income Tax Management Act
Value Added Tax Act
Social Security Act

Business and Administrative requirements:

e.g. Marketing
Billing and accounting
Customer Care and after sales service

Fix reasonable periods which can be justified with IDPC when required.

Data Subject to be informed of Retention Period at collection stage!

Powers of the Commissioner

Investigative powers

- enter and search any premises and access to all information;

Corrective powers

- warnings and reprimands; rectification or erasure; ban processing;
- administrative fines [effective, proportionate and dissuasive – up to €20 M];

Authorisation and advisory powers

- processing subject to prior checking; codes of conduct; certification bodies;
- advise the Parliament, Government and the general public;

Engage in legal proceedings

- Data Protection Appeals Tribunal; Court of Appeal - aggrieved from a decision;
- may institute proceedings in a Court of law against any person.

Organisational Challenges

- Identify current/new processing operations and map to a legal basis
- Increase awareness top – bottom approach
- Strengthen **Data Protection Structures**
- **DPO** (if applicable) needs to operate in accordance with GDPR
- Introduce DP by Design in systems
- Carry out DP Impact Assessments for processing operations
- Determine **retention periods**
- Prepare to give **“copy”** of data to data subjects when requested
- Prepare for dealing with **data breaches**

Final Key Messages

Continuity and change is of utmost importance

- **Compliance with current DP regime** is a very good start
- Organisations must identify **what is new and different** for them

IDPC is there to **help and guide** as necessary

IDPC is also there to **Regulate**

Ready – Steady - Go!