SYTORUS
DATA PROTECTION SPECIALISTS

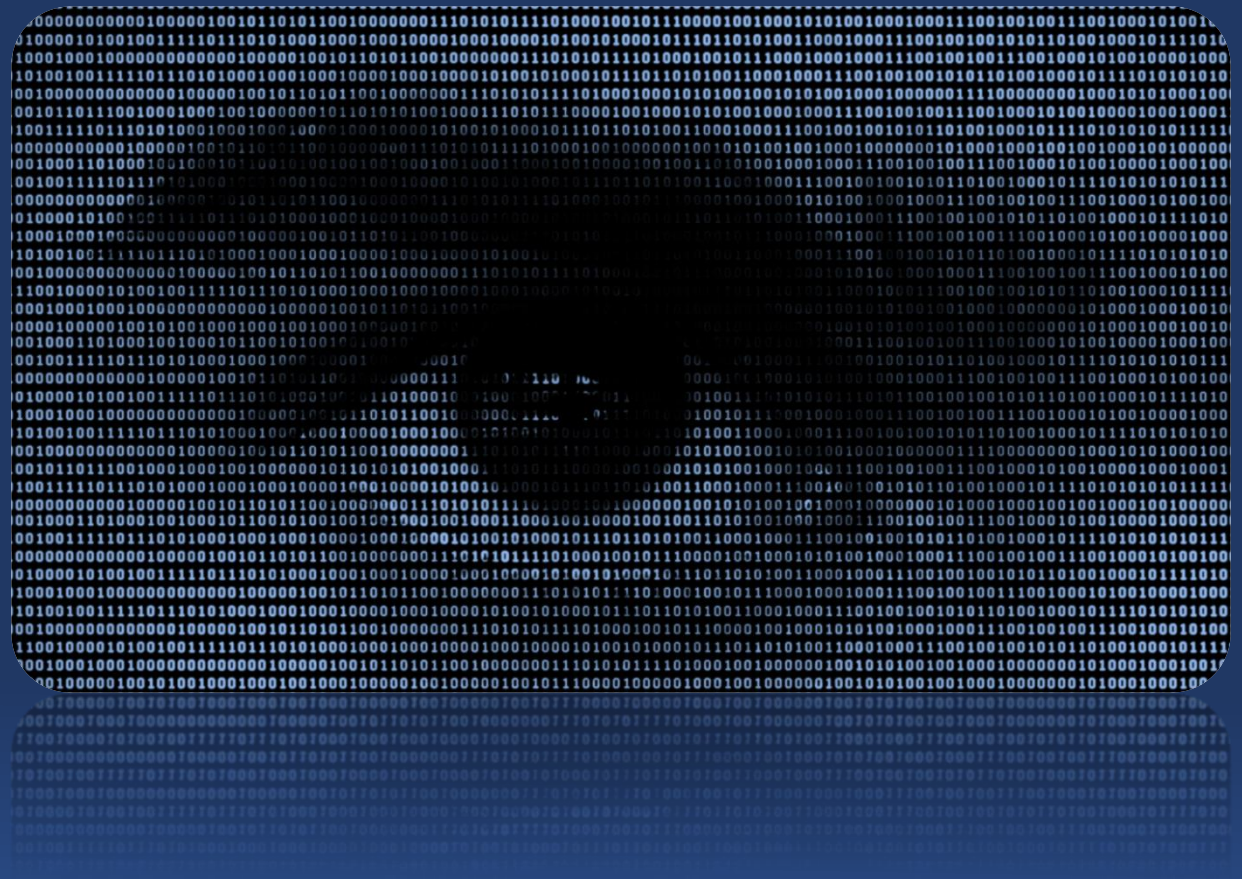
GDPR: An Introduction

Hugh Jones

© Sytorus Ltd.

Agenda

- Context of Privacy
- The Legislation
- Definition of Terms
- Data Management Principles
- The Data Subject Rights
- Supervisory Authority
- Offences
- Exemptions
- Sytorus Ltd. – who we are



© Sytorus Ltd.

Context

- Social
- Historical
- Technological
- Commercial

© Sytorus Ltd.

Data Protection & ‘the Brand’

© Sytorus Ltd.

Irish Data Protection Legislation

- Data Protection Act, 1988
- Data Protection (Amendment) Act, 2003
- Electronic Communications Regulation, 2011

© Sytorus Ltd.

Irish Data Protection Legislation

- Data Protection Act, 1988
- Data Protection (Amendment) Act, 2003
- Electronic Communications Regulation, 2011
- General DP Regulation 2018

© Sytorus Ltd.

Legislation - Electronic Communications Regulation (2011)

- Introduced the default ‘opt out’
- Active ‘opt in’ under three circumstances:
  - Pro-active Indication of interest
  - Prior purchase of product or service
  - A reasonable expectation of interest
- Distinction between servicing and marketing messages
- Prior, explicit consent for calls to mobiles
- Identification and provision of contact details
- All electronic marketing messages must include easy-to-use option to opt out
- Must use contact data at least once in a twelve-month period
  - “Use it or lose it!”

The GDPR does not apply where:

- Processing is in the course of an activity which falls outside EU law;
- Processing is being done by a natural person in the course of a purely personal or household activity (“domestic processing”);
- Processing by competent authorities for the purposes of
  - prevention, investigation, detection or prosecution of criminal offences,
  - the execution of criminal penalties,
  - the safeguarding against threats to public safety, and
  - the prevention of threats to public security

- Focus on ‘B2C’ correspondence, less emphasis on ‘B2B’

Some New Defined Terms

- 'Personal Data'
- ‘Sensitive Personal Data’
- 'Processing'
- 'Restriction of Processing'
- 'Profiling’
- 'Pseudonymisation'
- ‘Manual Filing System'
- 'Genetic Data'
- 'Biometric Data'
- ‘Cross-Border Processing’
- 'Main Establishment'
- 'Representative'
- 'Binding Corporate Rules'
- 'Supervisory Authority'

© Sytorus Ltd.

The Characters in the GDPR

- Data Subject
- Data Controller
- Data Processor
- Joint Controller
- Nominated Representative
- Data Protection Officer
- Supervisory Authority

- No exceptions for Volunteers!

The Data Management Principles of the GDPR

1. Fair, Transparent and Lawful Processing
2. Purpose Limitation
3. Minimisation of Processing
4. Data Accuracy/Data Quality
5. Retention, Storage Limitation
6. Security and Confidentiality
7. Liability and Accountability

© Sytorus Ltd.

Lawful Processing Conditions: Personal Data (Article 6)

a. The Data Subject has given ***consent*** to the processing of their personal data for one or more specific purposes;
b. The processing is necessary for the ***performance of a contract*** to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
c. The processing is necessary for compliance with a ***legal obligation*** to which the controller is subject;
d. The processing is necessary in order to protect the ***vital interests*** of the Data Subject or of another natural person;
e. The processing is necessary for the performance of a task carried out in the ***public interest*** or in the exercise of official authority vested in the controller;
f. The processing is necessary for the purposes of the ***legitimate interests*** pursued by the Controller or by a third party (Processor), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the data subject is a child.

(This does not apply to processing carried out by public authorities in the performance of their tasks.)

© Sytorus Ltd.

Lawful Processing Conditions: Sensitive Personal Data (Article 9)

- The Data Subject has given ***explicit consent*** to the processing of those personal data for one or more specified purposes; or
- The processing is necessary for the purposes of carrying out the obligations of the Controller or of the Data Subject in the field of ***employment and social security and social protection***; or
- The processing is necessary to protect the ***vital interests of the Data Subject or of another person*** where the Data Subject is physically or legally incapable of giving consent; or
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other ***non-profit-seeking body*** with a political, philosophical, religious or trade-union aim, in connection with its ethos and purposes; or
- The processing relates to personal data which are ***manifestly made public*** by the Data Subject; or

© Sytorus Ltd.

Lawful Processing Conditions: Sensitive Personal Data (Article 9)

- The processing is necessary for the ***establishment, exercise or defence of legal claims*** or whenever courts are acting in their judicial capacity; or
- The processing is necessary for reasons of ***substantial public interest***; or
- The processing is necessary for the purposes of ***preventive or occupational medicine***, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional; or
- The processing is necessary for reasons of public interest in the area of ***public health***, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or
- The processing is necessary for ***archiving purposes in the public interest***, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

© Sytorus Ltd.

Data Controller - Implications

- Data Processor Agreements
- Vendor Selection criteria
- Joint Controller Agreements (where relevant)
- Data Quality Review (including consent)
- Legal basis for processing activities
- Data Processing Logs
- Privacy Impact Assessments
- Breach Notification Obligation
- Retention Schedule
- Data Protection Officer (where mandated)
- Respect for Individual Rights

© Sytorus Ltd.

Data Processor Role

- Must be able to provide appropriate technical and organisational structures
- Must be able to demonstrate competence and compliance
- Can only engage sub-contractors with Controller's approval
- Controller has right to object to appointment of sub-contractors
- Data Processor contract must be in place, with prescribed clauses
- Same contract clauses and obligations will apply to sub-contractors
- Processor is primarily liable for failure of sub-contractors
- Where Processor determines the processing, they will be treated as a Controller for that proportion of the processing
- Must maintain a written (electronic) log of processing activities
  - Categories of processing
  - Transfers to third countries
  - Details of Controller on whose behalf the processing is carried out

© Sytorus Ltd.

Data Processor - Impact

- In order for the engagement between the Data Controller and Data Processor to be compliant, a formal, written contract must be in place prior to the processing taking place

- Since the Data Controller remains the primary entity responsible for compliance under the Regulation, the Data Controller can determine the parameters and scope of the processing being conducted by the Third Party.

© Sytorus Ltd.

Data Processor Contract

The contract must set out:

- The **subject-matter and duration** of the processing;
- The **nature and purpose** of the processing;
- The **type** of personal data and **categories** of Data Subjects; and
- The **obligations and rights** of the Data Controller.

© Sytorus Ltd.

Data Processor Contract

In particular, it should stipulate that the Data Processor shall:

- Process the personal data **only** **on the basis of documented instructions** from the data controller, including with regard to transfers of personal data to a country outside the EU;
- Ensure that persons processing the personal data have **committed themselves to confidentiality**;
- Take all appropriate measures to **ensure the security** of the personal data in proportion to the risk to which it will be exposed;
- Respect the data controller's preferences with regard to the **enlisting of another processor** or sub-contractor;
- Undertake to assist the Data Controller by **appropriate technical and organisational measures**, to fulfil the Data Controller's obligations towards the data subject's rights;
- Assist the Data Controller in ensuring compliance with its **obligations with regard to Data Breach Notifications**, **Privacy Impact Assessments** **and prior consultation** with the Supervisory Authority, where necessary;
- At the end of the provision of data processing services, **to delete or return all the personal data** to the Data Controller, and to delete existing copies unless EU or Member State law requires storage of the data; and
- To make available to the Data Controller all information necessary **to demonstrate compliance** **with the obligations laid down in the GDPR**, allowing for and contributing to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Controller.

© Sytorus Ltd.

Logging of Processing Activities

In order to demonstrate compliance with the GDPR, each Data Controller and Data Processor will be required to maintain a log or record of processing activities for which it is responsible.

Decision regarding Establishment

© Sytorus Ltd.

Logging of Controller Activities

That record should contain all of the following information:

- The name and contact details of the Controller and, where applicable, the Joint Controller, the Controller's Representative and the Data Protection Officer;
- The purposes of the processing;
- A description of the categories of Data Subjects and of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including Recipients in third countries or international organisations;
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation including the documentation of appropriate safeguards;
- Where possible, the envisaged time limits for erasure of the different categories of data;
- Where possible, a general description of the technical and organisational security measures.

© Sytorus Ltd.

Data Processor – Logging of Activities

The GDPR stipulates that the Processing Log to be maintained by the Data Processor must contain the following information:

- The name and contact details of the Data Processor or Subcontractor;
- The name and contact details of each Data Controller on behalf of which the Processor is acting;
- The details of the Controller's or the Processor's Nominated Representative;
- The details of the Controller's Data Protection Officer, if any;
- The categories of processing carried out on behalf of each Controller;
- Where the processing involves transfers of data to a third country outside the EU, the documentation of appropriate safeguards and, where possible;
- A general description of the technical and organisational security measures implemented by the Processor.

© Sytorus Ltd.

Breach Notification

The Controller is obliged to disclose any incident where the data is exposed to risk, even where the data may not have been disclosed outside the organisation or to an unauthorised individual

Information should be provided on the following aspects of the incident:

- A description of nature of the personal data breach;
- The categories and approximate number of Data Subjects concerned;
- The categories and approximate number of data records concerned;
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

© Sytorus Ltd.

Privacy Impact Assessment

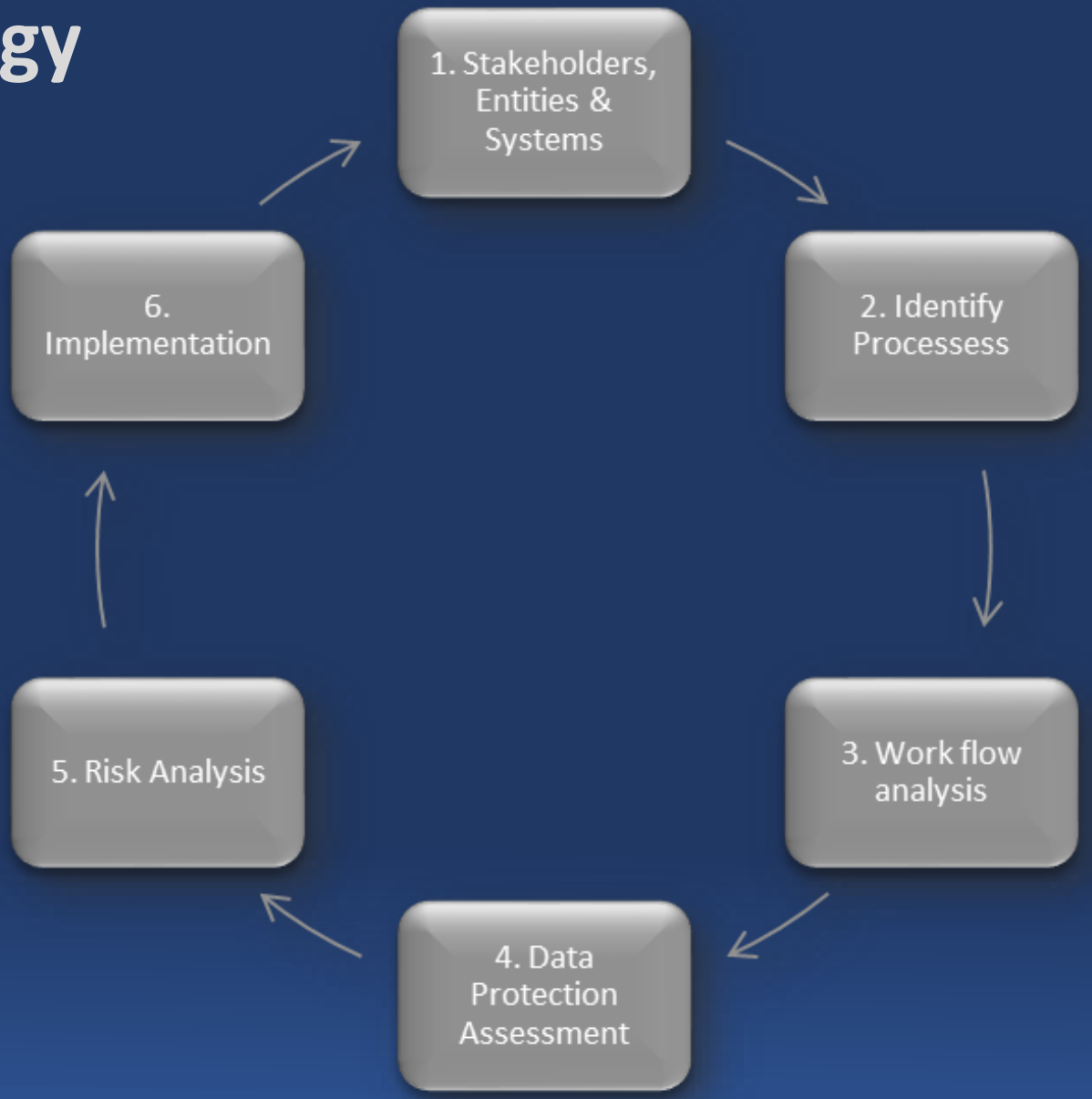
Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the Controller will be required to carry out a Privacy Impact Assessment in order to evaluate, in particular, the origin, nature, particularity and severity of that risk.

The following conditions and measures should be taken into account when determining the suitability and practice of a Privacy Impact Assessment:

- Where the personal data processing is likely to give rise to a risk to the data;
- Should involve the DPO and other, relevant stakeholders;
- Systematic evaluation of proposed processing;
- Identification of risk;
- Outline of the measures being taken to mitigate those risks;
- Outline of structures and measures planned to achieve compliance;
- Where substantial risk is identified, the Data Controller must check with the Supervisory Authority.

© Sytorus Ltd.

Privacy Impact Assessment: Methodology



© Sytorus Ltd.

The Data Subject's Rights

- The Right to be Forgotten (Right to Erasure)
- The Right to Restriction of Processing
- The Right to Object to Certain Processing
- The Right to Data Portability
- The Right of Access to One's Personal Data
- Rights in relation to Profiling and Automated Decision Making
- *30-day response time applies to all Data Subject Rights*

© Sytorus Ltd.

The DPO - Designation

- Where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or
- Where the core activities of the Controller or the Processor consist of processing operations which require regular and systematic monitoring of Data Subjects on a large scale; or
- Where the core activities of the Controller or the Processor consist of processing on a large scale of special categories of data such as data relating to medical, social welfare administration or criminal convictions and offences.

© Sytorus Ltd.

The DPO - Profile

- Expertise in the area of EU data protection law
- A good understanding of the way the organisation operates, with particular regard to its personal data processing activities; and
- An ability to interpret relevant data protection rules in that context
- Personal skills including integrity, initiative, organisation, perseverance, discretion, ability to assert himself/herself in difficult circumstances, an interest in data protection and the personal and professional motivation to be a DPO; and
- Interpersonal skills including communication, negotiation, conflict resolution and the ability to build strong, constructive working relationships
- Have the autonomy, related budget, necessary resources, signing authority and decision-making powers to execute data protection plans and tasks, address non-compliance issues, and report incidents to the relevant Data Protection Supervisory Authority without needing to refer 'up the line' for authorisation or permission to do so

© Sytorus Ltd.

The DPO - Role

- To inform and advise the organisation's management and employees who are processing personal data of their obligations under the Regulation;
- To keep them advised of their obligations with regard to other data protection provisions;
- To monitor the organisation's compliance with this Regulation and with the policies of the controller or processor in relation to the protection of personal data, including:
  - ✓ the assignment of responsibilities
  - ✓ awareness raising
  - ✓ training of staff involved in the processing operations, and
  - ✓ conducting timely and appropriate audits
- To provide advice where requested as regards the data protection impact assessment and monitor the compliant performance of any solution arising from a PIA;
- To cooperate fully with the respective Supervisory Authority;
- To act as the contact point for the Supervisory Authority on issues related to the processing of personal data, including prior consultation with the Supervisory Authority where necessary.

© Sytorus Ltd.

The DPO – Periodic Reporting

- The DPO should prepare a report, normally once or twice a year, to inform his/her organisation, and in particular the senior management team, of the status of the organisation's data protection compliance

- The reports could be published on the organisation's intranet site and a copy of these reports should be available to the Supervisory Authority, either by publication or by sending it to that Office directly

© Sytorus Ltd.

The DPO – Periodic Reporting

These reports could include:

- A status report on notifications, prior checks, and the state of the organisation's Risk Register;
- A summary of any supervision activities of the Supervisory Authority with respect to the organisation over the relevant period (audits, investigations, guidance, correspondence, etc.);
- Information on any staff training activities that were provided over the relevant period, and any training planned for the future;
- A status report on efforts undertaken to satisfy any recommendations made by the Supervisory Authority in any previous engagements;
- Report on requests and complaints received from data subjects, the organisation's response to date, and their current status; and
- The results of checks and audits carried out by the DPO in selected parts of the organisation using a rotation system, including conclusions as to the organisation's or department's state of compliance and, where necessary, recommendations to resolve situations of noncompliance.

© Sytorus Ltd.

Supervisory Authority - Role

Where a Data Controller does business solely within one Member State of the EU, they will abide by the decisions and enforcement of the Data Protection/Supervisory Authority in that jurisdiction.

- Investigation
- Formal Notices
- Enforcement
- Administrative Penalties
- Consistency

© Sytorus Ltd.

Less than 6 months To Go!

1. Becoming Accountable
2. What is meant when the GDPR refers to a ‘Legal Basis’
3. Processing Children’s Data
4. Using Customer Consent as Grounds to Process Data
5. Detecting and Reporting Data Breaches
6. Data Protection Impact Assessment and Privacy by Design
7. International Organisations and the GDPR
8. Data Protection Officer
9. Communicating with Staff and Service Users
10. Data Subject Rights
11. Will Access Requests Change?
12. Review of Data Processor Contracts

© Sytorus Ltd.

SYTORUS
DATA PROTECTION SPECIALISTS

End of Presentation

Thank-you!

© Sytorus Ltd.