GDPR

Understanding GDPR
Agenda

• Introduction to GDPR
• Key Principles and Actors
• Data Security Requirements
• Egosecure Philosophy
• Data POLICIES into PRACTICE
• How Egosecure supports GDPR strategies
• Conclusions
What is GDPR?

1. The General Data Protection Regulation (GDPR) replaces the EU’s existing Data Protection Directives 95/46/EC

2. It was adopted by the European Parliament Council in April 2016 and will be in effect on the 25th May 2018

3. Organisations processing Personally Identifiable Information (PII) of EU citizens have two years to comply
GDPR Principles

The Seven Data Protection Principles

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability
Penalties

• A fine of up to 10,000,000 EUR or 2% of global annual turnover maybe applied but can rise to 20,000,000 EUR and 4% of global turnover for serious breaches

• Data Controllers are liable for the financial penalties in cases where processing is found to be in breach of GDPR. Data processors are also liable if they act contrary to the instructions of the controller or if they do not comply with the GDPR specifics
<table>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish data privacy as a fundamental right</td>
<td>The GDPR considers data privacy as a fundamental right of an individual, which includes a “right to the protection” of their personal data. Anyone based in the EU, or anyone handling or targeting the personal data of an EU-based individual must have processes, technology, and automation to effectively protect personal data.</td>
</tr>
<tr>
<td>Clarify the responsibilities for EU data protection</td>
<td>The GDPR applies to anyone based in the EU, or anyone handling the personal data of an EU-based individual or targeting him/her by offering goods or services from outside the EU borders.</td>
</tr>
<tr>
<td>Elaborate on the data protection principles</td>
<td>The GDPR considers encryption as only one of the components of a broad security strategy, and mandates that organizations need to consider assessment, preventive, and detective controls based upon the sensitivity of the data they have.</td>
</tr>
<tr>
<td>Increase enforcement powers</td>
<td>EU aims to ensure the compliance with the GDPR by enforcing huge fines up to 4% of global annual revenue upon non-compliance.</td>
</tr>
</tbody>
</table>
Core Actors of the GDPR

Any enterprise that uses data belonging to a European Citizen must comply. It is vital to understand the actors in information usage within a global stage.

<table>
<thead>
<tr>
<th>Actor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Subject</td>
<td>An independent public authority established by a Member State such as court or auditing agency.</td>
</tr>
<tr>
<td>Personal Data</td>
<td>Any information, including sensitive information, relating to a Data Subject.</td>
</tr>
<tr>
<td>Controller</td>
<td>A natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of personal data. For example, a controller can be an organization or CIO.</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>An individual within the Controller with extensive knowledge on the data privacy laws and standards. Data Protection Officer (DPO) shall advice the controller or the processor of their obligations according to the GDPR and monitors its implementation. DPO acts as a liaison between the controller and the supervisory authority. A DPO for example can be a Chief Security Officer (CSO) or a Security Administrator.</td>
</tr>
<tr>
<td>Processor</td>
<td>A natural or legal person, agency or any other body which processes Personal Data on behalf of the Controller. For example, a developer, a tester, or an analyst.</td>
</tr>
<tr>
<td>Recipient</td>
<td>A natural or legal person, agency or any other body to whom the personal data is disclosed. For example, a tax consultant, insurance agent, or agency.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Any natural or legal person engaged in an economic activity. This essentially includes all organizations whether in public or private sector, whether in EU or outside of EU.</td>
</tr>
<tr>
<td>Third Party</td>
<td>Any natural or legal person, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data. For example, partners.</td>
</tr>
<tr>
<td>Supervisory Authority</td>
<td>An independent public authority established by a Member State such as court or auditing agency.</td>
</tr>
</tbody>
</table>
Key Security Requirements - 1

- Assess Security Risks – high risk information must be assessed in relation to the organisation’s processes, profiles and tools needed to safeguard the personal data.
- Prevent Attacks – GDPR recommends several techniques to prevent attack success
  - Encryption
  - Data anonymization and Pseudonymisation
  - Privileged user access control
  - Introduce file level control
  - Minimise the amount of data collected and retained
Key Security Requirements - 2

• Monitor and Detect Breaches
  – Audit data collection
    • GDPR requires recording or auditing on personal data and remain under the controller. A controller will maintain a record of processing of PII
  – Monitor and timely alert
    • In the case of a PII breach the controller must investigate it and report it to the supervisory authority within 72 hours.

• Quality of Protection
  – Centralisation – recommends centralising when dealing with security of multiple applications and systems.
  – **Data security by design** – make data protection the core of your security systems – let’s go into more detail on the next slide
  – Comprehensive Security – GDPR mandates protection of PII in all stages of the data lifecycle.
Key Requirements 3 - Data Protection by Design

- GDPR requires Data Protection by Design (Article 25)
- Data Protection by design is crucial to minimise privacy risks, promote privacy and data protection compliance from the start and establish trust
- Data Protection Impact Assessment (DPIA) are required to take the design approach – establish current state and record remediation steps.
- DPIAs can drive design for handling personal data

Define data security Requirements
- Initial DPIA Assessment
- Define requirements and gaps

Understand the data workflows
- Volume
- Internal/External
- Value
- Types

Understand the impact on individuals
- Regular DPIAs to assess impacts on individuals
- Review projects against requirements
Need Help?

• Guardian can help you:
  – to develop and deliver DPIAs with our comprehensive services
  – with software to analyse, protect and implement policies, eg EgoSecure
  – with methodologies for GDPR Compliance
  – methods for continuous compliance monitoring
  – GDPR integration into your risk management
EgoSecure’s Philosophy

**Control**
Removable Media Devices like USB sticks can be connected to any computer

**Audit**
This fact will not be registered, no traces will be left. It is not possible to track what data was copied

**Filter**
Any user can introduce any kind of content and software including games or malicious software and viruses

**Encryption**
Corporate confidential data can be copied to USB stick. Once it is lost or stolen – the data will be in the wrong hands

Management to manage every aspect of the behaviour in various business scenarios
Overview of Egosecure

AUDIT
- Audit

FILTER
- Content Analysis & Filter Antivirus

CONTROL
- Access Control
- Application Control

INSIGHT

ENCRIPTION
- Removable Device Encryption
- Full Disk Encryption
- Folder Encryption
- Network Encryption
- Cloud Encryption
- Mail Encryption
- Android Encryption
- iOS Encryption

MANAGEMENT
- Mobile Device Management
- Secure Erase
- Green-IT
**How Egosecure supports GDPR - 1**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Egosecure</th>
</tr>
</thead>
<tbody>
<tr>
<td>High risk information must be assessed in relation to the organisations</td>
<td><strong>Egosecure Insight</strong> watches, monitors, records all information movement</td>
</tr>
<tr>
<td>processes, profiles and tools needed to safeguarded the personal data.</td>
<td>activities that shows where the highest risks to information. It builds</td>
</tr>
<tr>
<td></td>
<td>a view of who is accessing, what are they accessing and when. However,</td>
</tr>
<tr>
<td></td>
<td>it cannot identify or classify information assets. Insight will</td>
</tr>
<tr>
<td></td>
<td>anonymise user identity when required.</td>
</tr>
<tr>
<td>Prevent Attacks – Encryption</td>
<td>Once <strong>Egosecure Insight</strong> identifies the highest risks the following</td>
</tr>
<tr>
<td></td>
<td>suite of modules can be added to protect the data:</td>
</tr>
<tr>
<td></td>
<td>• Network, folder and mail encryption</td>
</tr>
<tr>
<td></td>
<td>• Mobile Encryption (IOS, Android)</td>
</tr>
<tr>
<td></td>
<td>• Cloud Encryption</td>
</tr>
<tr>
<td></td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>• Removable Device Encryption</td>
</tr>
<tr>
<td></td>
<td>Encryption does not anonymise information but if data is encrypted then</td>
</tr>
<tr>
<td></td>
<td>it is useless to hackers</td>
</tr>
<tr>
<td>Data anonymization and Pseudonymisation</td>
<td>Encryption protects the data without the need for complex data</td>
</tr>
<tr>
<td></td>
<td>anonymization</td>
</tr>
</tbody>
</table>
## How Egosecure supports GDPR - 2

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Egosecure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged user access control</td>
<td>Egosecure can be used with other tools to manage access controls</td>
</tr>
<tr>
<td>Introduce file level control</td>
<td>Egosecure controls all external devices including flash drives, communication devices, smartphones and tablets. Control all types of interfaces - USB, Firewire etc. «Read only» mode for removable media.</td>
</tr>
<tr>
<td>Minimise the amount of data collected and retained</td>
<td>Egosecure cannot give statistics of data age, etc for retention policies but destroy data using Secure Erase.</td>
</tr>
<tr>
<td>Audit data collection</td>
<td>Track all user activity, access violations, file operations, shadow copies.</td>
</tr>
<tr>
<td>Monitor and timely alert</td>
<td>Potential breaches can be spotted before they happen with full analysis.</td>
</tr>
<tr>
<td>Quality of Protection</td>
<td>Egosecure covers internet, network, servers, cloud, storage, mobile, comms.</td>
</tr>
<tr>
<td>Centralisation</td>
<td>Egosecure console gives central visibility of information as it flows across the organisation. Help decisions on data centralisation of PII data.</td>
</tr>
<tr>
<td>Data security by design</td>
<td>Egosecure shows the greatest risks which can be addressed as a priority.</td>
</tr>
<tr>
<td>Comprehensive Security</td>
<td>Covers all channels, data at rest, in motion and in use.</td>
</tr>
</tbody>
</table>

*www.guardiantechnologies.co.uk*
Using Egosecure to Design Policy

Assess

- Execute initial DPIA
- Use Egosecure Insight to understand data flows, volumes to support DPIA activities
- Identify requirements based upon Insight results
- Identify top risks for prioritisation

Implement

- Build DPIA reviews regularly into regular risk processes
- Implement modules to protect PII data
- Review Insight to verify protection
- Write policies based upon successful implementation

Monitor

- Add protection where needed
- Update policies
- Run regular DPIAs to document processes and progress
- Verify with data controller regularly to establish trust maturity

Forensic analysis of data breaches
Egosecure Insight

A powerful analysis tool to identify areas of vulnerability

Detailed forensic analysis in case of a data breach
Summary

- Companies must review compliance and adherence to GDPR as soon as possible.
- Egosecure Insight will provide clarity on information security risks including PII information.
- Execute regular DPIAs to define roadmap of mitigation and proof of execution.
- High priority risks can then be addressed with appropriate modules quickly and easily.
- Centralisation of control through the same dashboard for all security measures.
- Full audit capability in the light of a breach.
- Be prepared for GDPR using Egosecure to manage your controls.
Contact Guardian Technologies to plan your steps to GDPR compliance

0330 223 0261
sales@guardiantechnologies.co.uk
www.guardiantechnologies.co.uk