Maintaining Compliance with the GDPR

Ian Grey
Information and Cyber Security consultant
ian.grey@wadiff-consulting.co.uk
https://www.linkedin.com/in/iangreyuk

Russell McDermott
Sales Engineer
Russell.Mcdermott@netwrix.com
+44 (0) 203 588 3023 x 2208
General Data Protection Regulation (GDPR)

25th of May 2018

- The Accountability principle
- How much training you need to give staff
- How to manage risks in the supply chain
- How to deal with incidents and data breaches
- What needs to be in place so data subjects can exercise their rights
WADIFF Consulting

- Ex-Operations Director, compliance with Data Protection Act
- More than 25 years experience in IT and technical areas, and holding board level posts for ensuring effective security measures are in place
- Experience in the commercial, public and not for profit sectors
- GDPR Practitioner
- ISO27001:2013 Lead Auditor

This is not legal advice
It depends...
How to Prepare

- Article 40 - Codes of conduct
- Article 42 - Certification

**Article 29 Working Party**

The article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines from complying with the requirements of the GDPR.

The Article 29 Working Party now expects that guidelines on certification will be adopted in early 2018.
The controller shall be responsible for, and be able to *demonstrate* compliance with the principles (Article 5)
processed lawfully, fairly and in a transparent manner in relation to the data subject

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

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

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

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The data controller shall be responsible for, and be able to demonstrate compliance with the principles

accountability

lawfulness, fairness and transparency

purposelimitation

storage limitation

integrity and confidentiality

accuracy

data minimisation
Accountability

- Maintain relevant documentation on processing activities (Article 30)
- Implement measures that meet the principles of data protection by design and data protection by default (Article 25)
- Use data protection impact assessments where appropriate (Article 35)
- Appoint a Data Protection Officer where appropriate (Articles 37-39)
- Implement appropriate technical and organisational measures
Accountability - Technical and Organisational Measures

- Policies
  - Information Security Management System (ISMS)
    - Access Controls
    - Anti-Virus and Vulnerability Management
    - Backup
    - Change Management
    - Classification & Handling
    - Training
  - Acceptable Use
  - Incident Management
  - Business Continuity
  - Internal audits of processing activities, policies and records
  - etc.
Accountability - Technical and Organisational Measures

- Internal audits – look for *evidence*
  - Access Control; new and suspended logins, group policies and membership
  - Password; enforces ‘strong’ passwords, are updated(?), 2FA
  - Anti-Virus and Vulnerability Management; updated virus definitions
  - Backup; no errors reported and restores work
  - Change Management; review documents, e.g. for backout and records kept for Projects
  - Classification & Handling; spot checks on paper and electronic records
  - Policies; reflect how the organisation works and legal requirements

- Security Certifications
  - Cyber Essentials
  - ISO27001
Information Security / Data Protection Training

- How much to give...and when
- Amount depends on the role of the individual – include temporary staff
- Give training an induction and at ‘regular’ intervals, keep records
- eLearning tools vs In person
Manage Risks in the Supply Chain

- Data mapping identifies where you obtain/share personal data with/from third parties

- Risks
  - From third party; no lawful basis to use the personal data
  - With third party; data breach, stored outside EU, sub contracted etc

- Sharing - contact third party and ask them questions about what they are doing to prepare for the GDPR
  - Large companies, e.g. Microsoft, have websites to answer questions
  - How quickly will they inform you if there is a suspected or actual data breach
  - If they store any personal data outside the EU
  - If they provide key services or process high risk data; examples of the ‘appropriate technical and organisational’ measures used to protect it

- Update contracts
Dealing with Incidents and Data Breaches

- Data breach – “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” (Article 4)

- This is where a Data Protection Officer needs to be involved (if you have one)

- Use your Incident Management policy. Does it present a risk to data subjects rights and freedoms?
  - No; record why it will not be reported, e.g. data is encrypted
  - Yes; report to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it (Article 33 has details of what information needs to be given)
    - If it is likely to result in a “high risk” also contact the data subjects (Article 34 has details of what information needs to be given)
# Data Subjects Exercising Their Rights

- **Do ID checks**

<table>
<thead>
<tr>
<th>Right</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be informed</td>
<td>Information at data collection points, Privacy notice</td>
</tr>
<tr>
<td>Access</td>
<td>“Subject Access request”, Redact details (where appropriate)</td>
</tr>
<tr>
<td>Rectification</td>
<td>Pass on details of changes where data has been shared</td>
</tr>
<tr>
<td>Erasure</td>
<td>Erase if no lawful basis to process it, pass on erasure request where data has been shared</td>
</tr>
<tr>
<td>Restrict processing</td>
<td>Does it meet one of the 4 criteria? Pass on restriction request where data has been shared, Lift restriction (if appropriate)</td>
</tr>
<tr>
<td>Portability <em>(Consent/Contract &amp; processing automated)</em></td>
<td>Export in a commonly used and machine-readable format</td>
</tr>
<tr>
<td>Object <em>(Public or Legitimate Interest)</em></td>
<td>Stop processing</td>
</tr>
<tr>
<td>Automated decision making and profiling</td>
<td>“not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects”</td>
</tr>
</tbody>
</table>
About Netwrix Auditor

A visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations, and access in hybrid IT environments. It provides security intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.
What GDPR Requirements Does Netwrix Auditor Address?

**CHAPTER II. Principles**

Article 5. Principles relating to processing of personal data
§1 (f); §2

**CHAPTER III. Rights of the data subject**

Article 15. Right of access by the data subject
§1 (b)

Article 16. Right to rectification

Article 17. Right to erasure (right to be forgotten)
§1

Article 20. Right to data portability
§1

**CHAPTER IV. Controller and processor**

Article 24. Responsibility of the controller
§1

Article 25. Data protection by design and by default
§1; §2

Article 32. Security of processing
§1 (b, c, d); §2; §4

Article 33. Notification of a personal data breach to the supervisory authority
§1 (b, c, d); §2; §4

Article 34. Communication of a personal data breach to the data subject
§1
Demonstration
How Can I Secure the Sensitive Data?

- Identifying owners of sensitive data
- Streamlining attestations of access rights to sensitive data
- Detecting unauthorised activity around your sensitive data
What About Data Subject Rights?

Addressing **subject access** requests and complying with the ‘**Right to Be Forgotten**’
What Else to Do for Compliance with Accountability Principle?

- Implementing **access control measures**
- Monitoring **what's going on** in your entire IT environment
- Capturing a **complete audit trail** of activity in information systems
How Should I Deal with Incidents and Data Breaches?

- Detecting **security incidents** in a timely manner
- Investigating anomalous activity and events that are detected
- Determining the **severity** of a **data breach**
Next Steps

Join the Q&A session and submit your questions here:
https://www.netwrix.com/achieve_and_maintain_compliance_with_the_GDPR.html#session-3

Contact Sales to obtain more information netwrix.com/contactsales

Data Classification: What It Is, Why You Should Care and How to Perform It

What is GDPR: 10 FAQs
https://try.netwrix.com/what-is-gdpr-ebook-nemea.html
Questions?

Thank You!

Ian Grey
Information and Cyber Security consultant
ian.grey@wadiff-consulting.co.uk
https://www.linkedin.com/in/iangreyuk

Russell McDermott
Sales Engineer
Russell.Mcdermott@netwrix.com
+44 (0) 203 588 3023 x 2208