GDPR

A service providers view

TTI Summer Forum – Getting to grips with GDPR

June 2017

Agenda

Why is GDPR different?

What does this mean for data processors?

Proving accountability requires auditable evidence created through appropriate measures

- What are appropriate organisational measures?
- What are appropriate security measures?

Assessing risk and how to mitigate it

Business and functional changes to consider

Why is GDPR different?

Basic principles

- GDPR makes it clear that the data subject owns any data which describes or identifies them
- They have the right to determine how it is used, check it and withdraw it
- Anyone who handles this data is held accountable and must be able to demonstrate how they protect it and what they do with it

GDPR - evolution not revolution

- Principles haven't changed but the requirements are now more explicit
- Uses a 'big stick' to ensure compliance

Risk

- Direct data processor accountability
- Poor data controller behaviour can cause reputational damage to data processor

Definitions

What does GDPR mean for data processors?

Key requirements for processors

PII must be processed with appropriate security or organisational measures to ensure protection against unauthorised or unlawful access and must be able to demonstrate compliance

- Article 5.1.f, and 5.2

A contract must be in place between the controller and processor stipulating responsibilities and where EU GDPR applies

- Article 28.3

Documented approval between the controller and processor is required for all processing activities

- Article 28.3.a

The processor must be able to demonstrate that employees are authorised to process PII and that these employees have committed to confidentiality

- Article 28.3b

PII = Personally Identifiable Information

Key requirements for processors

Appropriate technical and organisational measures must be in place to ensure that protection is by design and is the default

- Articles 25.1, 25.3 and 32.1

Records must be kept of what data is held, how it is protected and who is responsible for it

- Article 30

The supervisory authority must be notified within 72 hours of a breach if the data lost may put the rights and freedoms of a data subject at risk

- Article 33

A data privacy impact assessment must be performed prior to processing operations

- Article 35.1

GDPR emphasises accountability

Proving accountability requires auditable evidence created through **appropriate** measures

Principles relating to processing of personal data
Article 5.2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 5.1 (‘accountability’).

What are appropriate organisational measures?

Staff training

- GDPR and general InfoSec awareness
- Secure coding standards
- Information security policy

Information asset management

- **What** are you holding, **where** is it held, **who** is responsible for it - 3Ws

Information Security Management System (ISMS)

- Document how you approach InfoSec so that your organisation applies security controls in a consistent manner
- Document how you deal with security incidents

Incident and change management

- Ensure that you record all incidents, change and processing requests
- Ensure that all changes and processing requests are authorised by the appropriate personnel

What are appropriate security measures?

The obvious stuff (at least it should be)

- Make sure you have a firewall and the rules are regularly reviewed
- Ensure that servers are configured based on CIS hardening benchmarks and they only perform one role
  - Patch in a timely manner
  - Use managed anti-virus
  - Use a web application firewall to protect web sites
- Ensure that any hypervisor used for Virtualisation is patched and hardened
- Ensure that your network uses segmentation best practice
- Physical security matters
  - Minimise access to what should be secure areas
  - Monitor with CCTV
  - Stops theft, key loggers, unauthorised WiFi and many more !

What are appropriate security measures?

The stuff you may not have thought about

- Access control
  - No shared accounts
  - Enforce complex passwords
  - Account expiry
  - Multi factor authentication for sensitive areas
- Logs and log management
  - Consolidate all logs into a centralised environment
  - Ensure all systems and components use the same time source
- Event analysis
  - Analyse logs to spot un-usual activity
  - Automate security alerts
- Backups
  - Hardware failure
  - Human error
  - Ransomware

What are appropriate security measures?

Policies, procedures and processes

- Don’t forget your users and their devices
  - Do you have an acceptable use policy
  - Are devices regularly patched
  - Do devices have anti-virus
  - Do you use full disk encryption on devices in case they are stolen
  - Can you remote wipe phones & tablets if they are lost or stolen
  - Do you have an approved software list
  - Do you control and audit access into environments with GPDR PII data
  - Have you considered the risk that BYOD creates
- Leavers and Joiners
  - When staff leave, is their access from all systems revoked
  - When staff join are they security trained
  - When staff join or change roles, are their access rights reviewed

Assessing risk and how to mitigate it

Risk review

Start from the assumption that current protection of PII is not sufficient for GDPR compliance

Identify and document what you have - 3Ws
(if you don't know what you have, how can you protect it?)

- Information assets
- Infrastructure assets
- Policies, procedures and configuration guides

Apply data categorisation to all information assets

- Determine and document the confidentiality, integrity and availability needs of each information asset (CIA)

Ensure that documentation is up to date

- Configuration guides
- Policies and procedures
- ATCORE uses PCI DSS as a reference

Risk review

Audit infrastructure assets for each information asset

- Shows the risk against the CIA requirement
- Check against configuration guides
- Leads to a plan which highlights any infrastructure changes required

Data Privacy Impact Assessment

- Risk to the individual rather than the organisation
- Data controller risk but will require data processor support

External risks

- Assess customer readiness as a data controller
  - Need to manage upwards as data controller behaviour could compromise the data processor
- Assess supplier readiness as data processors
  - Especially important for dynamic packaging requirements
  - Commercial relationship can be complicated - data controller <-> external data processor

Business and functional changes to consider

Business and functional changes to consider

Encryption of PII

- DPIA will determine need - how is this achieved technically?

Hardening of Infrastructure

- Apply PCI like controls to all infrastructure in scope for PII

Data subject access and deletion

- How do you identify that the request is coming from the individual in question
- How is this managed, what was the basis for consent
- Are there any legal requirements to keep data

Data retention period

- Configurable date based on contract or determined by consent - anonymisation applied when no longer valid

Business and functional changes to consider

Data subject report and download request

- Probably PDF and/or XML - what needs to be provided, what about other pax on a booking

Management of basis for consent

- Need to distinguish between contractual and freely given consent including recording and reporting (includes where the consent came from)

There will be additional requirements based on customer requirements and guidance from Working Party 29 and the ICO

Some useful links

Reform of EU data protection rules

- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

EU Article 29 Working Party

- http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

UK Information Commissions Office - Data protection reform

- https://ico.org.uk/for-organisations/data-protection-reform/

Thankyou