
The Privacy Practice
Shining Light on Privacy Issues
Bytes ‘GDPR’ Compliance Summit

GDPR – a crash course in compliance

- The regulatory position – Old & new
- The changes
- What about Security
- The implications

What's GDPR all about?

- Brings privacy law up to date
- Applicable to all industries
- More stringent & structured than previously (at least in the UK)
- Covers all personal data

What is personal data?

- Personal data
  - Name, address, phone – Traditional view of data
  - IP address; company ID numbers; nicknames
  - Biometrics
  - Sensitive personal data
    - Race or ethnicity; political opinions; religious beliefs; Trade-union membership; genetic or biometric data; health; sex life or orientation; criminal convictions
- "information relating to an identified or identifiable natural person….directly or indirectly"

GDPR – What's the same?

- DPA 8 principles
  - Fair & lawful;
  - purpose limitation;
  - data minimisation;
  - accuracy;
  - storage limitation;
  - Subject rights;
  - Security;
  - International transfers

- EU Directive – DPA in UK
- Platform neutral

GDPR – What's the same?

- Still principles based, but now with added ingredients:
  - Fair, lawful & Transparent;
  - purpose limitation;
  - data minimisation;
  - accuracy;
  - storage limitation;
  - Security - integrity & confidentiality;
  - Accountability.
  - Subject rights – Separate chapter
  - International transfers – Separate chapter

- EU Regulation – directly applicable in the UK
- Still "platform neutral"

What's changed?

Transparency

- Level of information to data subjects increased dramatically
  - Specified information
  - Increased information for Subject Access Requests
  - Notice and consent

Accountability

- The ability to demonstrate compliance with the regulation
  - Specified documentation

Enhanced data subject rights

- Enlarged subject access rights; Right to erasure ("to be forgotten"); Right to correction; Data portability

What else will be effected?

- Legal Grounds for processing including Consent
- Privacy by Design and Default
- Data Protection Impact Assessments (DPIAs)
- Mandatory data breach notification
- One-stop shop
- International transfers
  - BCRs
  - Privacy shield
  - Model clauses, et al
- Processor liabilities
- Mandatory Data Protection Officers
- Fines - € 20 Million or 4% of Global turnover

What practical changes will it require?

- Can't be "left to legal"
- Embedded in operations
- Implication for technical architecture
- Increased importance for Information Security
  - Fines
  - Even greater press scrutiny & public awareness

What about Security?

Data Security in the General Data Protection Regulation

- Article 5

"shall be processed in in a manner that ensures appropriate security. … using appropriate technical and organisational measures".

- Article 32

"the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity"

What about Info Sec?

- Greater emphasis in the Regulation
  - Mention of security measures, including encryption
- Data Breach notification
- Privacy by Default
  - Privacy by Design
  - Data Protection Impact Assessments

Data Breach Notification

- **Notification dependent upon risk**
  - Three categories: No Risk; Risk; High Risk
- **Timing of SA notification**(DPA as was)
  - Notification must be sent to the DPA without undue delay and normally within 72 hours after discovery of the breach where that is feasible.
- **Notification to Data Subjects** – defined circumstances BUT reviewable by the SA
- **Data Breach systems** need to be robust, rehearsed and regularly reviewed.
  - Not if When

PbyD and Default & DPIAs

What do they mean?

- No definitions
- No codes (yet)
- All mandatory – DPIAs in defined circumstances
- Auditing of the outcomes of the DPIAs

- All need to be INTEGRATED into operations and into development, with pre-planned IS

How can security use this?

- Argument for resources enhanced
  - Fines
- Security has to be embedded in operations; processes; and architecture
- IS has to be reviewed and updated
- Mandatory Data Breach notification

- If data is the new gold you need a good bank!

Starting Points for an Action Plan

- Gap analysis against present & future legislation
- Find & identify your data
- Operations integration
  - DPIAs
  - Breach notification
  - Data architecture
  - Consent, DPO
- Identify your allies
- Integrate IS into company strategy


The Privacy
Practice
Contact
jlg@leatongray.com
Shining Light on Privacy