THE EU GDPR –
You Can't Afford Not To Be Ready

ARMA Atlanta
May 4, 2018

Richard Sheinis, CIPP-US
Hall Booth Smith, P.C.
13024 Ballantyne Corporate Place
Suite 625
Charlotte, NC 28270
www.hallboothsmith.com
rsheinis@hallboothsmith.com
(980) 859-0381 (direct dial)
(404) 345-0749 (mobile)
@SheinisCyberLaw

GDPR

Why?

Current Directive 95/46/EC allows for too much fragmentation in data protection across the EU.

- Each member state had their own "take" on the Directive.
- GDPR allows little room for Member States or supervising authorities to change regulation (i.e., age of majority, timing of appeal of enforcement action).

When?

The GDPR is to be effective May 25, 2018. There is no grace period or "grandfather" provision. Everyone has had 2 years to get ready.

GDPR

Key Points:

1. **Does It Apply to Me?**
   It does if:
   a. You are a data controller or data processor established in EU; or
   b. You are not in the EU but you process personal data of data subjects **who are in the EU** and **you offer goods or services to data subjects in the EU**, or monitor the behavior of data subjects in the EU.

- **How do you know if you are offering goods or services to data subjects in the EU?**
  - Look at factors such as language and currency.

GDPR

Does GDPR apply to you?

- Not sure? Let's evaluate
- GDPR applies, but I have not done anything yet.

Don't worry, we have a plan

(but you have to stay until the end of the presentation to hear it!)

GDPR

2. Expanded/New Definitions:

a. **Personal Data –** Includes location data, online identifiers, and technology identifiers.

b. **Pseudonymous Data –** Data that does not allow identification of individuals without additional information and is kept separate.

c. **Sensitive Data** – Includes genetic data and biometric data.

d. **Profiling** – Automated processing of personal data used to evaluate an individual's "personal aspects".

GDPR

3. Consent:

a. Must be a clear, affirmative act.
b. Must allow for separate consent for each use or processing of data.
c. Must be specific as to the exact purpose of the use or processing.
d. Request for consent must be unambiguous using clear and plain language.
e. Data subject must be told that can withdraw consent at any time.
f. Must be explicit for processing of sensitive personal data (usually an opt-in-tick box).

GDPR

4. Rights of Data Subjects:

a.The right to be informed.

Guests must be told the following:

1. Identity and contact details of the controller and the data protection officer
2. Purpose and lawful basis for processing the data
3. The legitimate interests of the controller or third-party where applicable
4. Any recipient or category of recipients of the personal data
5. Details of transfers to other countries and safeguards in place

GDPR

6. Retention period
7. The existence of each data subjects' rights
8. The right to withdraw consent at any time where relevant
9. The right to lodge a complaint with a supervisory authority
10. The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences

GDPR

b. **The right of access**
c. **The right to rectification**
d. **The right to erasure**
e. **The right to restrict processing**
f. **The right to data portability**
g. **The right to object**

5. **Accountability:**
   - Data controllers must ensure compliance with the general data processing principles

GDPR

6. **Recordkeeping:**
   - No longer have to register with DPA.
   - Controllers and processors must monitor internal records of all data processing activities.

7. **Safeguards:**
   - Controller must implement appropriate technical and organizational measures, which are designed to integrate necessary safeguards into processing and compliance with the GDPR (including policies).

GDPR

8. **Data Protection Impact Assessment:**
   - Must perform a data protection impact assessment prior to processing data if processing likely to result in a high risk to the rights of individuals due to new technologies or the nature, scope, context and purposes of processing. (Supervising authorities must create a list of the kind of processing operations that require an impact assessment.)
9. **Data Protection Officer:**
   - Must have DPO if engage in regular and systematic processing of data subjects on a large scale.
   - A single DPO can serve more than one operation.

GDPR

10. Contract Between Data Controller and Data Processor

- Article 28 requires specific contractual language.

11. Data Breach Notification:

a. Notify affected individuals without undue delay if breach is likely to result in a **high risk** to the rights and freedoms of individuals.

b. Notify data protection authorities within 72 hours unless breach is unlikely to result in a **risk** to the rights and freedoms of individuals.

GDPR

12. Enforcement:

a. Supervisory authorities have investigative and corrective powers, and may impose fines of up to €20 million or up to 4% of worldwide annual turnover, whichever is greater.

b. Lesser sanctions include warnings, reprimands, ordering compliance with the GDPR, and **temporary bans on processing**.

c. There are three (3) tiers of penalties, but even the lowest tier has potential fines up to €10 million or 2% of turnover.

GDPR

Amount of fine should consider:

- Prior non-compliance penalties.
- Damage to data subjects (although the amount of the fine should not be an award of specific compensation for the damages suffered).
- The number of data subjects affected.
- Whether the non-compliance was the result of negligence or willful misconduct.
- Actions by the controller or processor to remediate the non-compliance or mitigate damages.
- Whether the entity had the appropriate technical, organizational and administrative measures in place.
- How the incident became known to the supervisory authority, i.e., was it self-reported.

GDPR

13. Data Transfer to Third Countries:

a. If Commission decides third country ensures an adequate level of protection; or

b. Other safeguards in place:

- BCR
- EU Model Contract Clauses
- Privacy Shield; or

c. Consent

GDPR

13. Right of Compensation:

Data subject can receive compensation from the Controller or Processor for damages suffered. Controller or Processor not liable if prove not in any way responsible for the event giving rise to the damage.

(Wonderful, now they can sue, just like in the U.S.!)

GDPR

Plan?

I. Initial Assessment
- Review company's services
- Develop data flow map for personal data collected or processed by the company
- Review company's advertising and marketing
- Review vendor contracts

GDPR

II. Initial Compliance Phase

- Identify gaps in GDPR compliance
- Amend/update contracts with data processors/vendors to be GDPR compliant
- Update company's privacy policy
- Update consent mechanisms used by the company to obtain or use data for purposes for which consent is required
- Assess the potential need for any data privacy impact assessments
- Identify the need for policies and procedures to meet GDPR requirements
- Assess technical and organizational measures in place
- Assess the need for a data protection officer
- Develop a plan to have mechanisms in place to assess data subjects exercise of rights granted by the GDPR

GDPR

III. Full and Final Compliance
- Implement required technical and organizational measures
- Institute training programs for staff compliance with GDPR
- Confirm that all data governance policies and controls are in place
- Develop a breach notification plan (should such notification ever be necessary)
- Develop a record keeping plan to maintain all records required by GDPR
- Confirm all compliance gaps have been addressed

Data Protection Weekly

provided by Richard Sheinis

April 11, 2018

Featured Article

Ransomware Takes Malware Mantle in Verizon Data Breach Investigations Report
ZDNet

The report is based on 53,308 security incidents, 2,216 data breaches and 67 contributors globally. Ransomware started to appear in 2013 and has become the top variety of malicious software and found in 39 percent of cases where malware was identified. In addition, attacks are moving to more ...

Richard Sheinis

Hospital CEO Forced to Pay Hackers in Bitcoin Now Teaches Others How to Prepare for the Worst
CNBC

It was a late Thursday in January when hospital administrator Steve Long was notified that his computer systems had just been hijacked by an unidentified criminal group. The hackers gave Long seven days to pay a ransom — or else. It was at the height of flu season, and a winter snowstorm was ...

Consumer Reports Reaches $16.4M Settlement in Michigan Data Privacy Case
Insurance Journal

The publisher of Consumer Reports magazine has reached a $16.375 million settlement of a lawsuit claiming it violated Michigan privacy law by selling readers' subscription and personal data to third parties without their consent. A preliminary settlement of the proposed class-action case against ...

Dem Senator to Introduce New Data Privacy Law Amid Cambridge Analytica Scandal
The Hill

All of the bill's conditions would be enforced by the Federal Trade Commission (FTC). Lawmakers in both chambers will press Zuckerberg on Facebook's data privacy and data collection practices on Tuesday. The high-profile hearing could have impacts on data regulation for the entire internet industry ...

How Blockchain Could Solve the Internet Privacy

GDPR