FOLEY HOAG AARPI

Setting Security Strategies and Getting Real About GDPR

MassTLC CISO Roundtable

Catherine Muyl, cmuyl@foleyhoag.com
Colin J. Zick, czick@foleyhoag.com

February 6, 2018

FOLEY HOAG AARPI

Colin J. Zick

Partner, Chair, Privacy and Data Security Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.

- Advises on issues involving the transfer of data between jurisdictions, including GDPR, EU-US Privacy Shield, and other relevant data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.

- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com. Serves as a member of Law360's Privacy & Consumer Protection editorial advisory board.

Catherine Muyl

Partner, Head of the French IP/IT Practice

Paris | +33 1 70 36 61 30 | cmuyl@foleyhoag.com

- Head of the Paris IP/IT practice.
- Works for French public entities and US and European private entities (ranging from start-ups to major international groups) on IT contracts and data protection issues, including GDPR and the transfer of data from the EU to the US. Regularly contributes to the firm's "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com.
- Represents State-owned companies and private entities in IP and IT disputes before the French courts and the EUIPO (European Union Intellectual Property Office).
- Experience working on cross-border litigation.
- Native language French, fluent in English, proficient in German.

New Obligations Starting May 2018

EU Data Subjects' Rights

- Information
- Access
- Rectification
- **Erasure ("the right to be forgotten")**
- Restriction
- **Data portability**
- Objection

What information does the data controller have to provide to data subjects?

- **Identity and contact details of the controller** and (if not established in EU) its representative,
- Contact details of the **Data Protection Officer**, where applicable,
- **Purposes** of the processing,
- If the controller intends to **transfer** personal data to a third country : the existence or absence of an adequacy decision by the Commission, which safeguards have been put in place and how to get a copy,
- **Period** for which the personal data will be **stored**,
- **Existence of the data subject's rights** (access, rectification, erasure, restriction, objection or data portability).

New Obligations Starting May 2018

Representative:

- Controllers and processors not established in the EU must appoint a representative in the Union.

Data Protection Officer:

Must be appointed where :

- Processing is carried out by a **public** authority or body; or,
- Core activities consist of processing operations which by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**; or,
- Core activities consist of **processing on a large scale of sensitive data**.

New Obligations Starting May 2018

Notification of data breach:

To the Supervisory Authority

Level: where it is likely to result in a risk to the rights and freedoms of individuals.

Without undue delay, no later than 72 hours

Content of notification:

- Nature of the breach
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

To Data Subjects

Level: where a breach is likely to result in a high risk to the rights and freedoms of individuals.

Without undue delay

Content of notification:

- Nature of the breach in clear and plain language
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

New Obligations Starting May 2018

Agreements between controllers and processors

- Heavier obligations and potential liabilities for processors.

- Contracts between controllers and processors are now mandatory and must include:
  - the subject matter and duration of the processing;
  - the nature and purpose of the processing;
  - the type of personal data and categories of data subjects;
  - the obligations and rights of the controller;
  - a list of minimum terms, obligations of the processors to ensure that both the controller and the processor comply with GDPR.

Mandatory record of processing activities

- Obligation to maintain a **record of processing activities** containing the answers to the following questions:
  - ❑ Who?
  - ❑ Where?
  - ❑ What?
  - ❑ Until when?
  - ❑ Why?
  - ❑ How?

Data Protection Impact Assessment

- Required where a processing likely to result in a high risk to the rights and freedoms of natural persons, for example:
  - processing on a large scale of sensitive data,
  - systematic monitoring of a publicly accessible area on a large scale (in particular CCTV),
  - automated processing on which decisions are based that produce legal effects.

Transfer of Data to Non-EU Countries

Transfers to countries which do not provide an adequate level of protection (including the US) :

- Current transfer tools :
  - to the US : Privacy Shield.
  - Standard Contractual Clauses (SCC) issued by the Commission.
  - Binding Corporate Rules.
  - Consent.

- Additional transfer tools as from May 2018:
  - SCC issued by a Supervisory Authority.
  - Code of Conduct approved by the Supervisory Authority with binding and enforceable commitments from data importer.
  - Certification with binding and enforceable commitments from data importer.

FOLEY HOAG AARPI

Thank you!

FOLLOW US: @FoleyHoag

www.securityprivacyandthelaw.com