NCOIL 2018 Summer Meeting

GDPR: Impact on Insurance Companies

JUDY SELBY

JUDY SELBY CONSULTING LLC

Judy Selby

- Judy Selby is the principal of Judy Selby Consulting LLC. She provides strategic advice to companies and corporate boards concerning insurance, cyber security, and regulatory/legal compliance. She also helps companies select appropriate insurance coverage for today's complex cyber threats and serves as an expert witness in insurance coverage disputes.
- Prior to her move to consulting, Judy practiced law for almost 25 years, handling large litigations and international arbitrations. She founded her former law firm's eDiscovery and technology practice as well as its information governance team, assisting clients to efficiently manage massive and complex data sets in today's challenging litigation and regulatory environments. Judy has spoken around the world about cutting edge cyber, privacy, insurance, and litigation issues, translating complex technical, legal and compliance issues into understandable terms.
- She has been quoted in leading publications, including the Wall Street Journal, Fortune, and Forbes, and authored the eBooks "Demystifying Cyber Insurance: 5 Steps to the Right Coverage" and "Big Data for Business Leaders: What Today's Decision Makers Need to Know." Judy completed courses in Finance with Harvard Business School HBX, Big Data, Crisis Management/Business Continuity, Cyber Security and the Internet of Things (IoT) with the Massachusetts Institute of Technology (MIT), Professional Education, Cloud Computing with the IEEE, and EU GDPR Data Protection Officer Training with Advisera.

General Data Protection Regulation

AN OVERVIEW

GDPR Principals: Accountability

- Lawfulness, fairness, and transparency
  - Don't hide anything from data subjects
- Purpose limitation
  - Collect personal data only for a specific purpose
- Data minimization
  - Process data only if it is necessary for a specific purpose
- Accuracy
  - Reasonable steps to erase or rectify inaccurate and incomplete data
- Storage limitation
  - Delete data when it's no longer necessary for the purpose for which it was collected
- Integrity and confidentiality
  - Only principal addressing security
  - Deliberately vague about security measures

Data subject rights

- Right to information
- Right to access
- Right to rectification
- Right to withdraw consent
- Right to object
- Right to object to automated processing
- Right to be forgotten
- Right to data portability

Why insurers must care

PROCESSING DATA IS A FUNDAMENTAL PART OF THE BUSINESS OF INSURANCE

How insurers process data

- Risk analysis
- Claims analysis and payment
- Detecting fraud
- Employee data
- Marketing

Important obligations under GDPR

Lawful Processing of Personal Data

Insurers must always have an appropriate legal basis for processing personal data.

GDPR identifies 6 legal grounds for processing, including consent.

More restrictive rules for processing of Special Categories of personal data.

Adequate Notice to Data Subjects

Before processing personal data, insurers must provide data subjects with detailed information, including who is processing the data and for what purpose.

This also applies to personal data obtained from a third party.

Respond to Data Subject Rights

Insurers must respond to data subject requests within 30 days.

Creates difficult operational and technical challenges.

Important obligations under GDPR

Manage Service Providers

Ensure that existing and new third party service providers that process personal data have instituted appropriate measures to comply with GDPR.

Done through contract and service level agreements.

Appoint a Data Protection Officer

Required if the insurer's core activities involve regularly monitoring individuals or the processing of special categories of data.

DPO monitors compliance with the Regulation, is the point of contact with the supervisory authority, and reports to the highest level within the company.

Privacy by Design and Default

Insurers must consider data protection when designing products.

Must be documented.

When a system, process, or service includes choices about how much information an individual wants to share, default setting must be the most privacy-friendly.

Important obligations under GDPR

Data Protection Impact Assessment

Insurers must conduct a risk assessment of proposed processing activity that is likely to result in a high risk to data subject rights.

Must be done before processing takes place.

If high risks are identified, insurer must consult with the supervisory authority.

Cross Border Data Transfers

To transfer personal data outside of the EU/EEA, insurers must make sure that the target company is based in a country that has adequate data protection rules.

Alternatively, insurers can rely on standard contractual clause or binding corporate rules.

The data subject may provide consent for the transfer.

Data Breach Notification

Three types of data breach:

- Confidentiality
- Availability
- Integrity

72-hour deadline to notify the supervisory authority.

Individuals must be notified if the breach creates a high risk to the rights of the data subjects.

Fines and Penalties: The Criteria

- Nature of infringement
- Intention
- Mitigation
- Preventative measures
- History
- Cooperation
- Data type
- Notification
- Certification
- Other

Two levels of fines

- Lower Level
  - Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher.
- Higher Level
  - Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.

Data subject remedies for GDPR violations

- Data subjects have the right to an effective judicial remedy if their rights have been infringed as a result of non-compliance with the Regulation.
- Any person who has suffered a material or non-material damage as a result of an infringement of the Regulation has the right to receive compensation from the data controller or the processor.

Insurance Coverage for GDPR Exposures

A second level of risk for insurers

- Overview of coverage issues

GDPR coverage issues

- Coverage for all three types of personal data breach
- Coverage for violation of EU regulation and actions by EU regulators
- Coverage for non-data breach exposures under the GDPR
- Coverage for fines and penalties
- Coverage for directors and officers

Questions?

Judy Selby

Principal

Judy Selby Consulting LLC

Judyselbyconsulting@gmail.com

917-270-8440

@judy_Selby