SEYFARTH SHAW

The GDPR Provisions Effective May 25, 2018: What Should Organizations Be Doing Now?

Presented by Scott Carlson, Jason Priebe, and Natalya Northrip

SEYFARTH SHAW

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Agenda

01 Transitioning from EU Data Privacy Directive to the EU GDPR

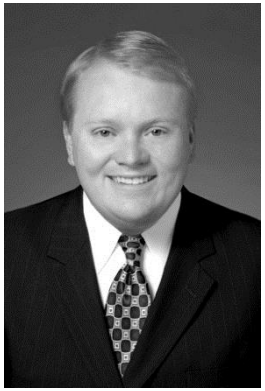
02 The GDPR Penalties

03 New Rights for Individuals Under the GDPR

04 Data Protection Officers

05 Heightened Auditing and Compliance Requirements

Speakers



Scott Carlson

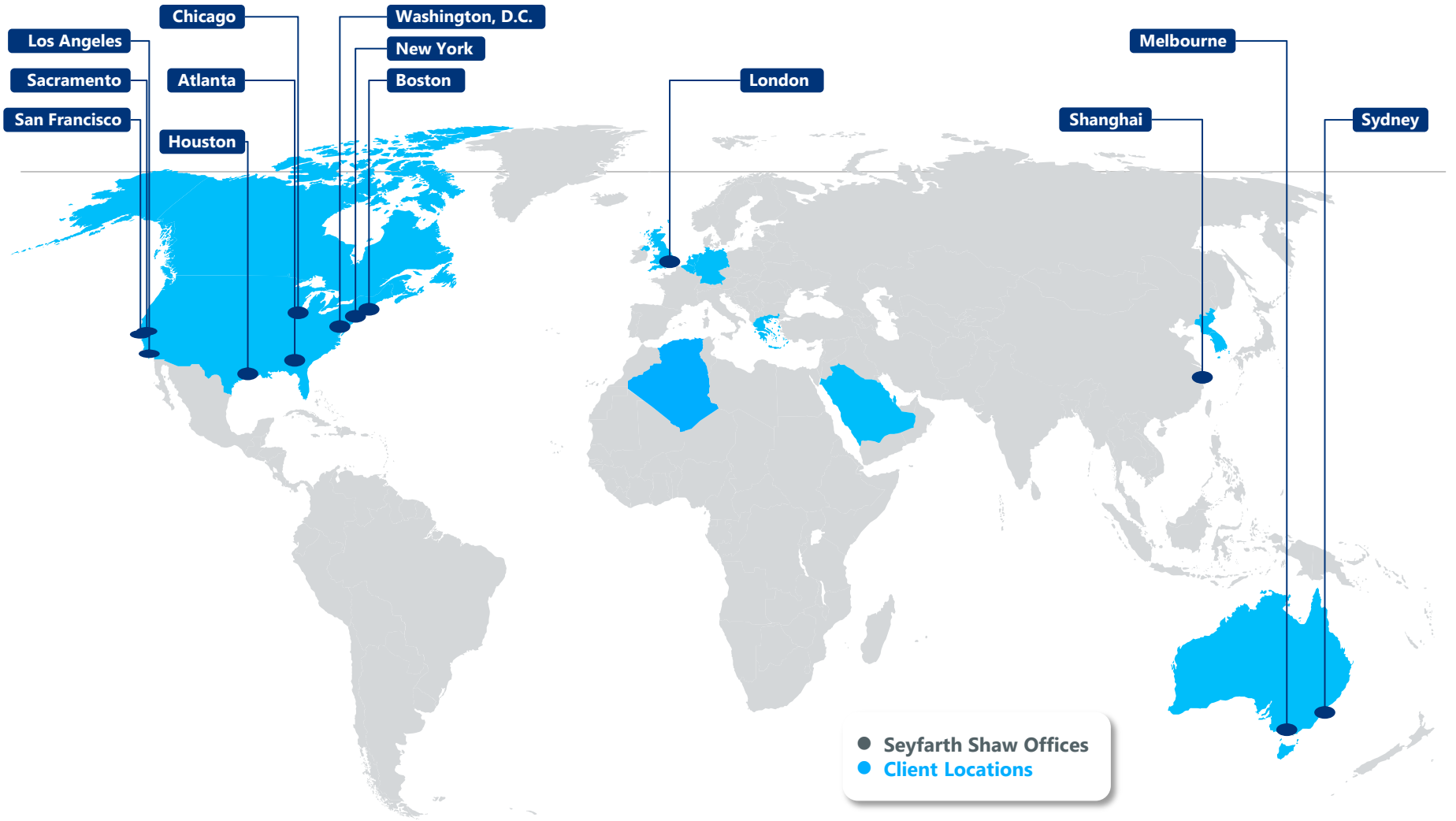
Partner,
Co-Chair Global Privacy and Security Team
Chicago Office
scarlson@seyfarth.com

Jason Priebe

Partner
Global Privacy and Security Team
Chicago Office
jpriebe@seyfarth.com

Natalya Northrip

Counsel
Global Privacy and Security Team
Chicago Office
nnorthrip@seyfarth.com



United States
Alabama
Alaska
Arizona
Arkansas
California
Colorado
Connecticut
Florida
Georgia
Hawaii
Idaho
Illinois
Indiana
Iowa
Kansas
Kentucky
Louisiana
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
Nebraska
Nevada
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota
Ohio
Oklahoma
Oregon
Pennsylvania
Rhode Island
South Carolina
South Dakota
Tennessee
Texas
Utah
Vermont
Virginia
Washington
West Virginia
Wisconsin
Wyoming

Australia
Bahrain
Belgium
Canada
Germany
Greece
Korea
Netherlands
Saudi Arabia
United Kingdom

Transitioning from EU Data Privacy Directive to the GDPR

	Directive 95/46/EC	GDPR
Authority	Required Member States to implement its principles through national legislation	GDPR is the law in all Member States; no national implementation is required
Application	Applies to data controllers only	Applies to data controllers, processors, and sub-processors
Enforcement	Inconsistent enforcement from state to state; low penalties	Bet-the-company sanctions
Data Protection Officers	Not required	Required for companies meeting certain criteria (under which most large companies will qualify)
Consent	Varying types of consent	Explicit consent only
Definition of Personal Data	Limited	Expanded to include location data, online identifiers, and genetic data
Data Privacy Impact Assessment	Suggested	Required when collecting and processing sensitive or great in volume personal data
Privacy Notice	Required with suggested language	Required with specific language
Breach Notification	Not required	Required within 72 hours

SEYFARTH SHAW

The EU General Data Protection Regulation (GDPR) Penalties

The GDPR Penalties

- The General Data Protection Regulation (GDPR) 2016/679 will enter into force on May 25, 2018.
- The GDPR brings dramatically increased penalties for data privacy violations.
- Tiered fines:
  - 10,000,000 Euros or 2% **Global** Turnover
    - Violations in data security, storage, breach, breach notification, trans-border transfers, transparency of information, child consent.
  - 20,000,000 Euros or 4% of **Global** Turnover
    - Violations in data processing, consent, data subject rights, third-party transfers

SEYFARTH SHAW

72-Hour Data Breach Reporting

72-hour Data Breach Reporting

- Under the GDPR, breach notifications are **mandatory:**
  - to the local Data Protection Authority (DPA) within 72 hours; and
  - to the affected data subjects "without undue delay."
- **UNLESS** the breach "is unlikely to result in a risk for the rights and freedoms of individuals" (e.g., anonymized or encrypted data).
- Any data-breach investigation and resulting determination regarding reporting must be documented.
- Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

72-hour Data Breach Reporting

- Minimize personal data at collection stage.
- Do not keep personal data longer than required under the retention policy or legal hold.
- Update the retention policy and records retention schedule.
- Critically evaluate each retention period for each record category.
- Have a designated and trained Security Incident Response Team (SIRT) in place.
- Establish individual notification procedures.

SEYFARTH SHAW

Privacy by Design as a Default Requirement

Privacy by Design and Default

- Article 25 requires controllers to implement “data protection by design and by default” requirements, including:
  - appropriate technical and organizational measures both at the time of the determination of the means for processing and at the time of the processing itself, and to integrate the necessary safeguards into the processing.
  - by default, process only personal data which are necessary for each specific purpose of the processing, including the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Privacy by Design and Default

- Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.
- Appropriate notice to data subject as to what data is being collected and why, with the right to opt out.
- Ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle:
  - building new IT systems for storing or accessing personal data;
  - developing legislation, policy or strategies that have privacy implications;
  - embarking on a data sharing initiative; or
  - using data for new purposes.

“Privacy By Design” Example – Connected Vehicles

- The French Data Protection Authority (CNIL) guidance for connected vehicles to address the privacy by design principle.
- Preferred scenario:
  - **“IN ⇒ IN”**: the data collected in the vehicle remain in the vehicle without the transmission to a service provider.
- Compliance more challenging in these scenarios:
  - **“IN ⇒ OUT”**: collected data are transmitted for processing to a service provider.
  - **“IN ⇒ OUT ⇒ IN”**: collected data are transmitted for processing to a service provider to trigger an automatic response in the vehicle.

Privacy by Design and Default – Practical Implications

- Develop and implement a Privacy Impact Assessment tool for the Business to complete each time it designs or procures a new data-processing system.
- Analyze data collection forms (e.g., web pages) to ensure that only data necessary for the purpose is collected.
- Automate data deletion processes, in accordance with your organization's records retention schedule, to ensure that personal data is automatically deleted at the end of its lifecycle.
- Analyze third-party data processor contracts to address how responsibility and liability for the implementation of "privacy by design" and "privacy by default" requirements will be addressed.

SEYFARTH SHAW

The “Right to be Forgotten” (i.e., Right of Data Erasure)

The Right to Be Forgotten - Scope

- Under Article 17 of the GDPR, the data subject shall have the right to obtain from the controller the **erasure** of personal data concerning him or her without undue delay, under certain circumstances, including where:
  - The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - The data subject withdraws consent for / objects to processing, and no other legal ground for processing applies;
  - The personal data have been unlawfully processed

The Right to Be Forgotten - Scope

- Where the controller has made the personal data that needs to be erased public, the controller "shall take reasonable steps" to **inform** other controllers that of the requested erasure
  - Consider suppliers, partners, resellers, customers.
  - Not an absolute requirement – may take into account available technology and the cost of implementation.
- In practical terms, data controllers will be required to erase a subject's data from ALL repositories.
  - Not an easy task (simply hitting "delete" unlikely to achieve compliance).
  - Consider encryption (deleting the key will render data unreadable).

The Right to Be Forgotten - Exceptions

- This is NOT an unconditional right.
- Continued processing permitted where it is necessary for:
  - exercising the right of freedom of expression and information;
  - compliance with a legal obligation;
  - reasons of public interest in the area of public health;
  - the establishment, exercise or defense of legal claims.

The Right to Be Forgotten – What Organizations Need to Do Now

- Prepare process and procedures for responding to erasure requests.
- When receiving an erasure request, evaluate whether compliance is required (i.e., are you permitted to continue processing because of an exception).
- Revisit your contracts with third-parties to obligate them to assist you in handling erasure requests with respect to personal data you transferred to them.
- Document each erasure request, investigation, and resolution.

SEYFARTH SHAW

The Right of “Data Portability”

Right to Data Portability - Scope

- The new **right to data portability** – a data subject's right to receive his/her personal data and to move and store it for further personal use on a private device, or to transmit that data to another controller.
- This right facilitates data subjects' ability to easily move data from one IT environment to another (enhanced competition)
- To fall within the scope of data portability, processing operations must be based on:
  - the data subject's consent or
  - a contract to which the data subject is a party (e.g., the titles of books purchased by an individual from an online bookstore).

Right to Data Portability - Scope

- Data portability applies only to data processing that is “carried out by automated means.”
  - Does not apply to paper files.
- Data portability covers the subject’s personal data that he or she *provided* to a data controller.
  - Includes data actively and knowingly provided by the data subject (e.g., mailing address, user name, age) and observed data that is “provided” by the data subject by virtue of the use of the service or the device (e.g., search history, location data).
  - Does not include “inferred” data, i.e., data generated by the subsequent analysis of the data subject’s behavior.

Right to Data Portability - Format

- The data should be provided “in a structured, commonly used and machine-readable format” that supports re-use.
- Data controllers are expected to offer a direct download opportunity for the data subject but should also allow data subjects to directly transmit the data to another data controller.
- Data controllers are expected to provide as many metadata with the data as possible to preserve the precise meaning of exchanged information.

Right to Data Portability – Retention, Notice, Timing

- **Retention:** No obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period.
- **Notice:** Data controllers are required to inform the data subjects regarding the availability of the new right to portability.
- **Timing:** Data controllers must answer a portability request "without undue delay" and in any case "within one month of receipt of the request"
  - 3 months for complex cases, but inform data subject of the delay within 1 month of the original request.

Right to Data Portability – Fees, Security

- **Fees:** Data controllers are prohibited from charging a fee for the provision of the personal data,
  - unless the requests are manifestly unfounded or excessive, "in particular because of their repetitive character."
- **Security:** When transferring data, the data controller is responsible for taking "all the security measures" needed to ensure that personal data is securely transmitted (e.g., by use of encryption) to the right destination (e.g., by use of additional authentication information).

Right to Data Portability – What Organizations Need to Do Now

- Review and update your current procedures.
  - How long to locate (and correct or delete) the data from all locations where it is stored?
  - Who will make the decisions about deletion?
  - Can your systems respond to the data portability provision of the GDPR, if applicable where you have to provide the data electronically and in a commonly used format?

SEYFARTH SHAW

Data Protection Officers

Data Protection Officers – When Required

- The GDPR requires some, but not all, companies to appoint a Data Protection Officer ("DPO").
- A DPO is required for the private sector in two specific cases:
  - Where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; and
  - Where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses.

Data Protection Officers – Core Activities

- Core activities of a controller relate to “primary activities and do not relate to the processing of personal data as ancillary activities.” (GDPR, Recital 97.)
- Core activities are the key operations necessary to achieve the controller’s or processor’s goals, e.g.:
  - processing patients’ health records by a hospital;
  - processing of surveillance information from private shopping centers and public spaces by a private security company.

Data Protection Officers – Large Scale

- “Large-scale processing operations” are operations that “aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk.” (GDPR, Recital 91.)
- WP29’s factors for consideration:
  - the number of data subjects concerned;
  - the volume of data and/or the range of different data items being processed;
  - the duration, or permanence, of the data processing activity; and
  - the geographical extent of the processing activity.

Data Protection Officers – Regular and Systematic Monitoring

- “Regular” means ongoing, recurring, or repeated at fixed times
- “Systematic” means occurring according to a system, pre-arranged, organized, or carried out as part of a strategy.
  - Examples include:
    - operating a telecommunications network,
    - profiling and scoring for purposes of risk assessment (e.g., credit scoring, fraud prevention),
    - location tracking (e.g., by mobile apps), and
    - monitoring of wellness, fitness and health data via wearable devices, CCTV, connected devices.

Data Protection Officers – Qualifications

- Expert knowledge of data protection law and practices.
  - Level of expertise must be commensurate with the sensitivity, complexity and amount of data an organization processes.
- Expertise in national and European data protection laws and practices.
- In-depth understanding of the GDPR.
- Necessary levels of organizational seniority, autonomy, and influence in order to play a key role in fostering a data protection culture within the organization and help implement essential elements of the GDPR.
- The DPO may have other functions within the organization, as long as they do not result in a conflict of interest.

SEYFARTH SHAW

Heightened Documentation of Compliance and Audit Requirements

GDPR Auditing and Compliance

- The GDPR will be enforced more strictly than the current Data Protection Directive.
- Prepare to demonstrate compliance (record keeping).
- Understand your obligations, current processes, and identify gaps.
- The EU Data Protection Authorities (DPAs) are increasing their budgets and workforce to police GDPR compliance.
  - E.g., the Irish Data Protection Commissioner (DPC) announced a 59% budget increase and plans to double its staff.

GDPR Auditing and Compliance

- Before May 2018, complete organizational self-audit and privacy assessment.
- Understand your obligations, depending on your role (controller or processor) in every GDPR area, including:
  - Personal data being processed (sensitive data, children's data)
  - Grounds for processing (consent, other lawful grounds)
  - Transparency requirements (updated privacy policy, notification of data subjects)
  - Purpose limitation, data minimization, accuracy, retention limitation

GDPR Auditing and Compliance

- Prioritize your audit by focusing on higher-penalty items first:
  - Consent
    - How collected and demonstrated?
    - Procedures for withdrawal
  - Data subject rights
    - Access to personal data; data portability; erasure and rectification; right to object; profiling and automated processing
  - Third-party transfers
    - Update transfer mechanisms

SEYFARTH SHAW

Thank You