Breaching Borders: Understanding the General Data Protection Regulation (GDPR)



Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS, Faculty, Harvard

Shannon Yavorsky, Partner, Orrick, Herrington & Sutcliffe LLP

(c) 2023 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown author is licensed under CC BY.

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.



Soliciting speakers is strictly prohibited.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Founder, Law & Forensics
Neutral, JAMS
Faculty, Harvard



Shannon Yavorsky
Partner, Orrick,
Herrington & Sutcliffe
LLP

(c) 2023 Lexeprint Inc. All Rights Reserved.

Agenda

- Introduction to the General Data Protection Regulation (GDPR)
- GDPR Obligations for the Data Controller and Processor
- GDPR Data Transfers
- GDPR Liability, Fines, and Class Actions
- Key Takeaways and What Lies Ahead

(c) 2023 Lexeprint Inc. All Rights Reserved.



Introduction to the General Data Protection Regulation (GDPR)

(c) 2023 Lexeprint Inc. All Rights Reserved.

What is the Purpose of the GDPR?

(c) 2023 Lexeprint Inc. All Rights Reserved



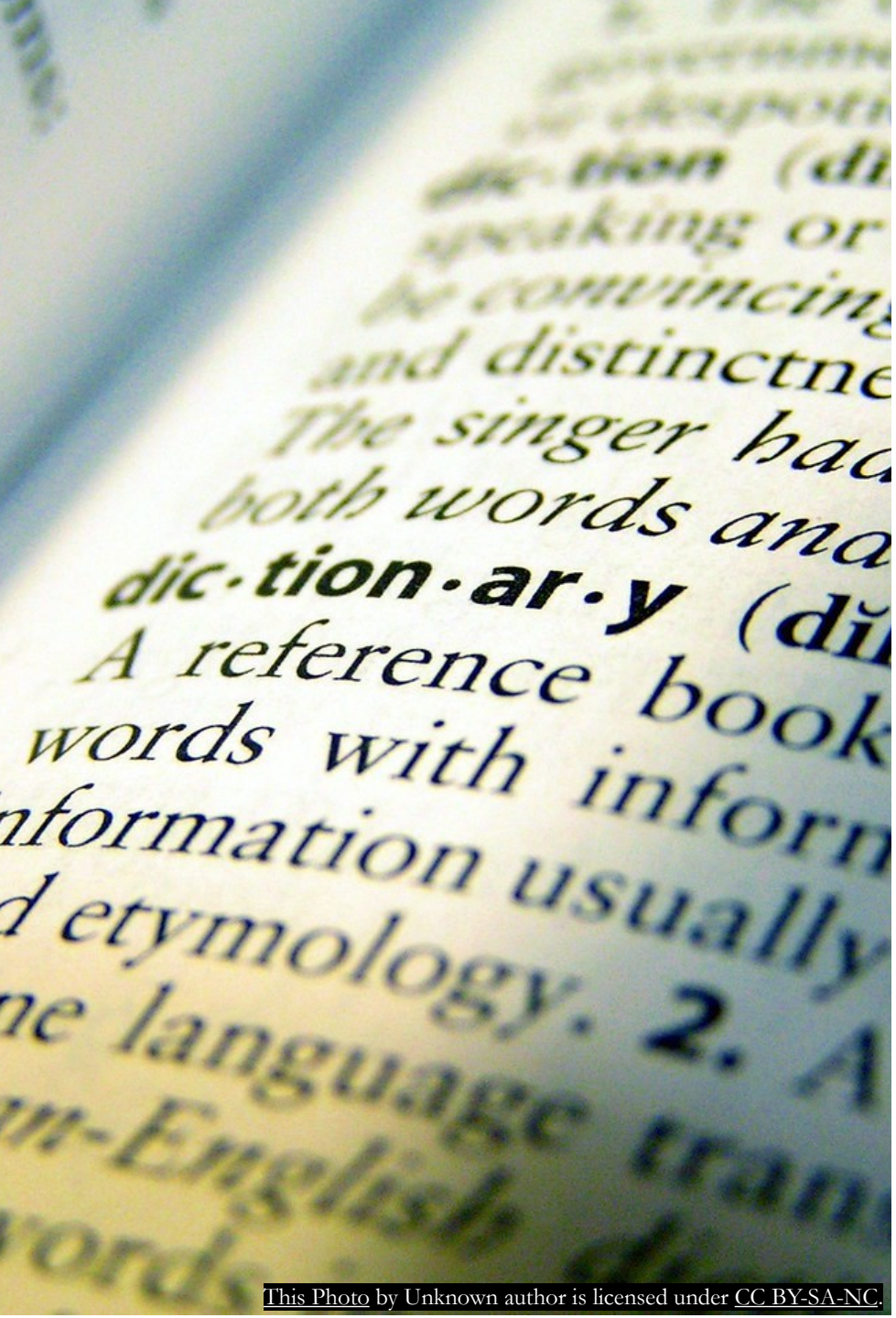
This Photo by Unknown author is licensed under CC BY-SA-NC.

What is the GDPR?

- The General Data Protection Regulation (GDPR) is an EU data privacy law that went into effect May 25, 2018.
- "It is designed to give individuals more control over how their data is collected, used, and protected online. It also binds organizations to strict new rules about using and securing the personal data they collect from people."*
- The GDPR replaced the 1995 Data Protection Directive, which created data protection laws on a country-by-country basis, resulting in a less cohesive patchwork of regulations in Europe.

* https://gdpr-info.eu/

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Key Definitions from the GDPR

- **Personal Data:** any information relating to an identified or identifiable natural person, also known as a data subject.
- **Data Subject:** a natural person who can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.*
- **Data Processing:** any operation which is performed on personal data or on sets of personal data by automated means. Data processing includes practices such as data collection, recording, organization, structuring, storage, alteration, retrieval, consultation, erasure or destruction.

* Article 4, GDPR

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC.

Material and Territorial Scope of the GDPR

- GDPR applies to the "processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."*

  * Article 2, GDPR

- The GDPR applies to processing:
  - In the context of an establishment in the EU; and
  - By a data controller or data processor not established in the EU but has data subjects in the EU that relates to:
    - The offering of goods or services to such data subjects; or
    - The monitoring of the behavior of data subjects.*

  * Article 3, GDPR

(c) 2023 Lexeprint Inc. All Rights Reserved.



Exemptions from the GDPR

Exemptions concerning:

- The processing of personal data.
- Freedom of information and expression.
  - The GDPR does not apply to personal data processing concerning activities for journalistic, academic, or artistic purposes.*
- Public interest and health.
  - The GDPR excludes data processing that is "necessary for reasons of public interest" in terms of "protecting against serious cross-border threats to health and ensuring a high equality of health" or for "archiving, scientific or historical research purposes" based on Member State law.
- Criminal prosecution.
  - The GDPR is not applicable to personal data processing used for the purposes of averting, investigating or prosecuting criminal activity. This includes protecting and preventing threats to public security.*

* Article 9, GDPR

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC.

Data Subject Rights under the GDPR

The GDPR provides the data subject with eight explicit rights under Art. 15-22. These are the:

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability;
- Right to object; and
- Rights around automated decision making and profiling.

(c) 2023 Lexeprint Inc. All Rights Reserved.



GDPR Obligations for the Data Controller and Processor

This Photo by Unknown author is licensed under CC BY.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Do Corporations Outside of Europe Need to Comply with the GDPR?

(c) 2023 Lexeprint Inc. All Rights Reserved



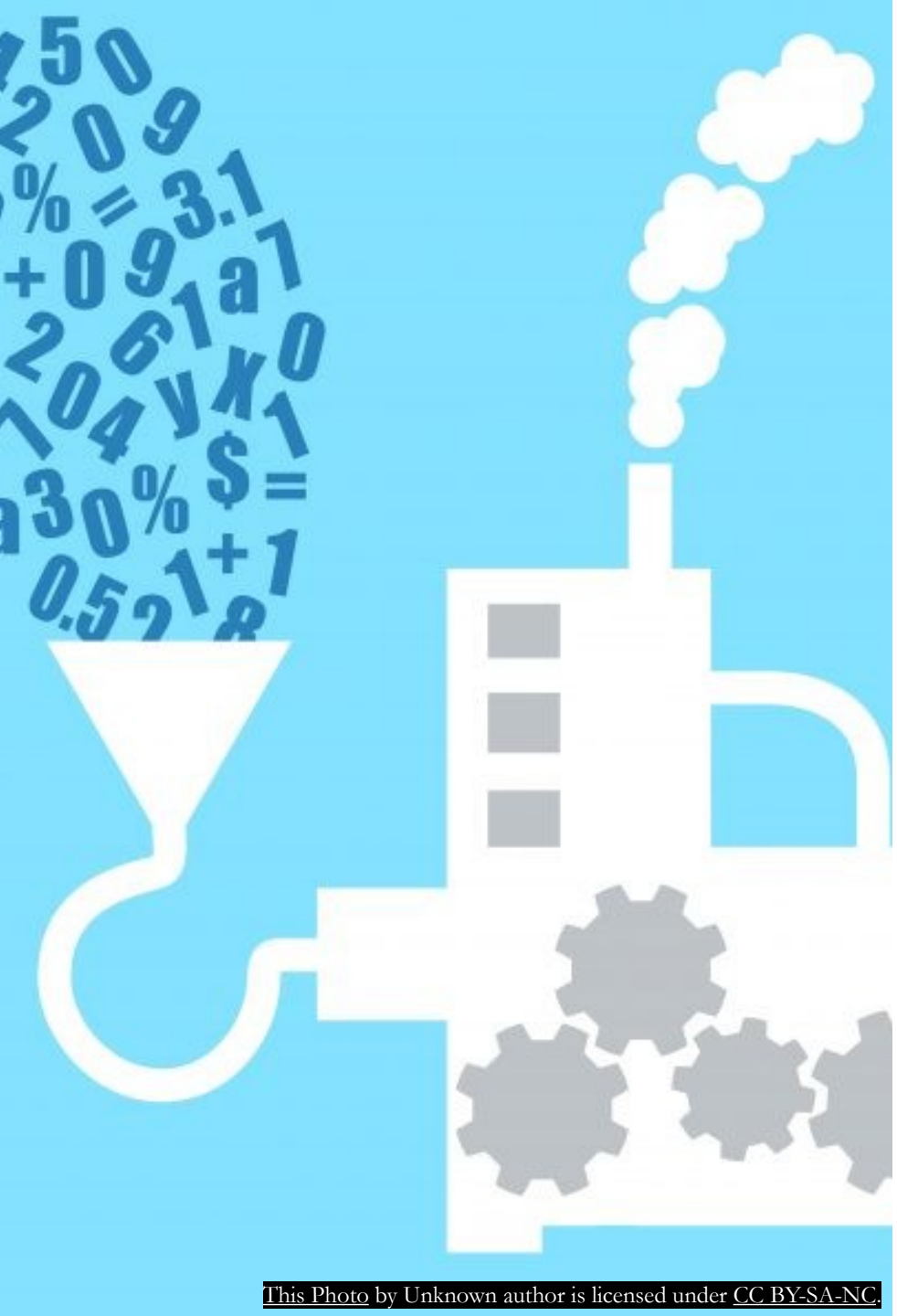
Data Controller

Data Controller: The entity which determines the purposes and means of the processing of personal data.

Obligations (GDPR Article 24)

- Take into account the purpose, nature, context, and scope of the data processing activities.
- Assess the appropriate level of security, taking into account the likelihood of risks presented by processing the data to the freedoms and rights of any natural persons.
- Implement appropriate technical organizational and technical and security measures that demonstrate that the data processing activities comply with the GDPR.
- Ensure any person acting under the controller or the processor only process the instructions from the controller.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Data Processors

Data Processor: An entity which processes personal data on behalf of the controller.

Obligations (GDPR Article 28)

- Process only personal data according to the data controller's documented instructions unless otherwise required by law.
- Implement appropriate organizational and technical procedures to meet GDPR requirements.
- Abide by sub-processor requirements

(c) 2023 Lexeprint Inc. All Rights Reserved.



Seven Principles of the GDPR

Data processors must act in accordance with seven protection and accountability principles outlined in Article 5.1-2 of the Act:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Data Protection Officer

- **Data Protection Officer (DPO)**
  - A DPO must provide expert professional knowledge in data protection law and IT security (the scope depends on the complexity of data processing and the size of the company).
- **What are the duties of a Data Protection Officer? (Article 37)**
  - (1) Informing and advising the organization and its employees about their GDPR obligations and other data protection laws;
  - (2) Monitoring compliance, such as managing internal processes and advising on Data Protection Impact Assessments (DPIAs); and
  - (3) Facilitating the relationship with the supervisory authority and the individuals whose data is processed.

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Privacy by Design & Privacy By Default

Privacy by Design

- Data controllers and processors are required to go beyond technological solutions, security procedures regarding data handling should be under consideration and implemented from day one.
- The Regulation details utilizing best practices in data minimization, pseudonymization, and process documentation.

Privacy by Default:

- .Measures must be taken by default to ensure that only the personal data necessary for each specific business purpose is processed, this entails taking data protection measures as the rule, not the exception
- In practice, companies must have a well-defined data lifecycle that ends with the destruction of said data and additional information must be actively requested from the data subject.*

** Article 25, GDPR*

(c) 2023 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown author is licensed under CC BY-SA-NC.

Data Protection Impact Assessment (DPIA)

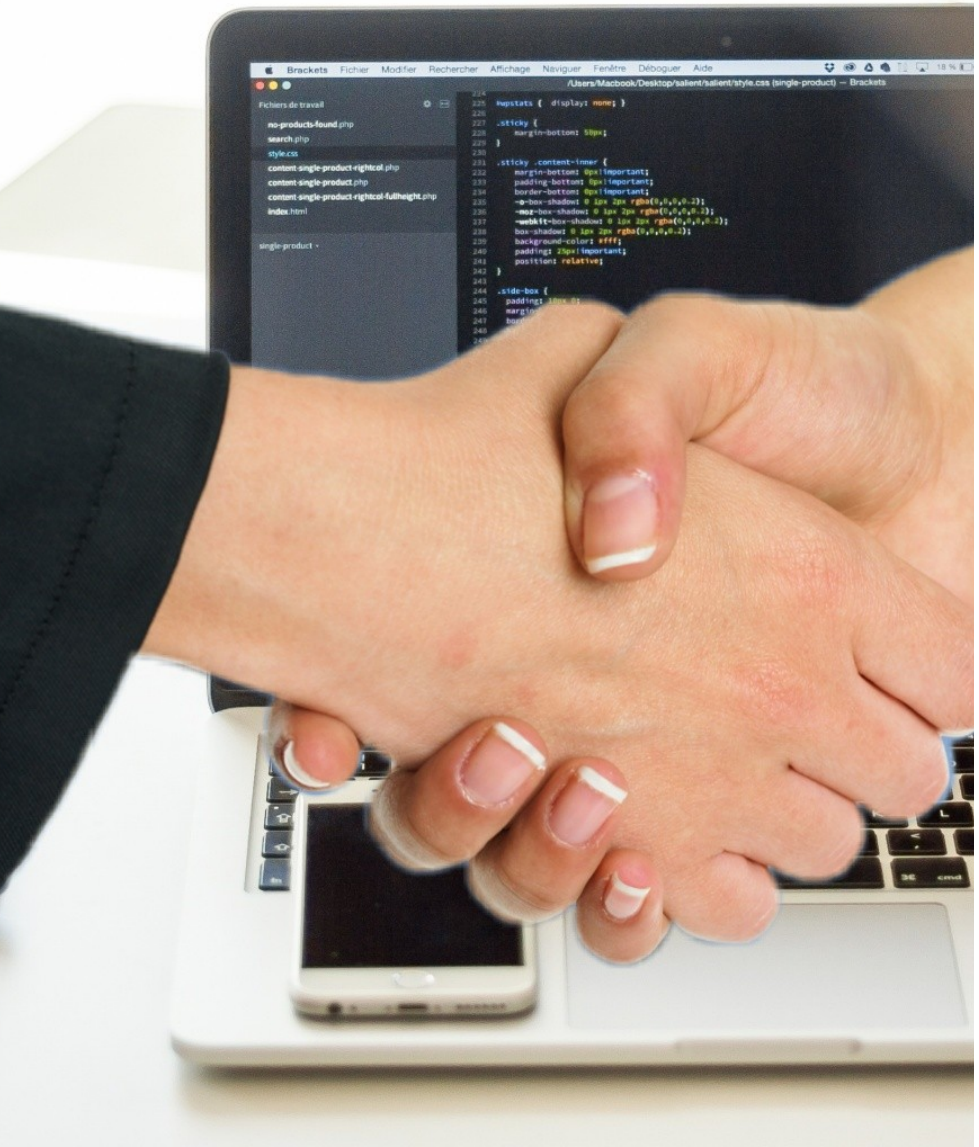
Data Protection Impact Assessment (DPIA) (Article 35)

- Required under the GDPR any time an organization begins a new project that is likely to involve "a high risk" to other people's personal information.*
- DPOs support Data Controllers in fulfilling this obligation.

What the DPIA must include:

- A systematic description of the envisaged processing operations; including the purposes of the processing and, where applicable, the legitimate interest pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes; and
- An assessment of the risks to the rights and freedoms of data subjects.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Data Processing Agreement (DPA)

- The GDPR requires data controllers to sign a Data Processing Agreement (DPA) with any parties that act as data processors on their behalf.
- DPAs are legally binding contract that states the rights and obligations of each party concerning the protection of personal data.
- A DPA must include the:
  - Subject of processing;
  - Duration of processing;
  - Purpose for processing;
  - Type of personal data involved; and
  - Categories of data subject.*

* Article 28, GDPR

(c) 2023 Lexeprint Inc. All Rights Reserved.



What are the Legal Bases for Data Processing?

Article 6 outlines the instances in which it is legal to process personal data. The Article details that personal data processing, including the collection and storage of data, is prohibited unless it can be justified with one of the following conditions:

1. Unambiguous consent to process the data.
2. Necessary to execute or to prepare to enter into a contract.
3. Necessary to comply with a legal obligation.
4. Necessary to save somebody's life.
5. Necessary to perform a task in the public interest or public function.
6. Legitimate interest to process someone's personal data. *

*The fundamental rights and freedoms of the data subject may override this interest in certain circumstances which require protection of personal data, in particular when the subject is a child.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Article 6, GDPR



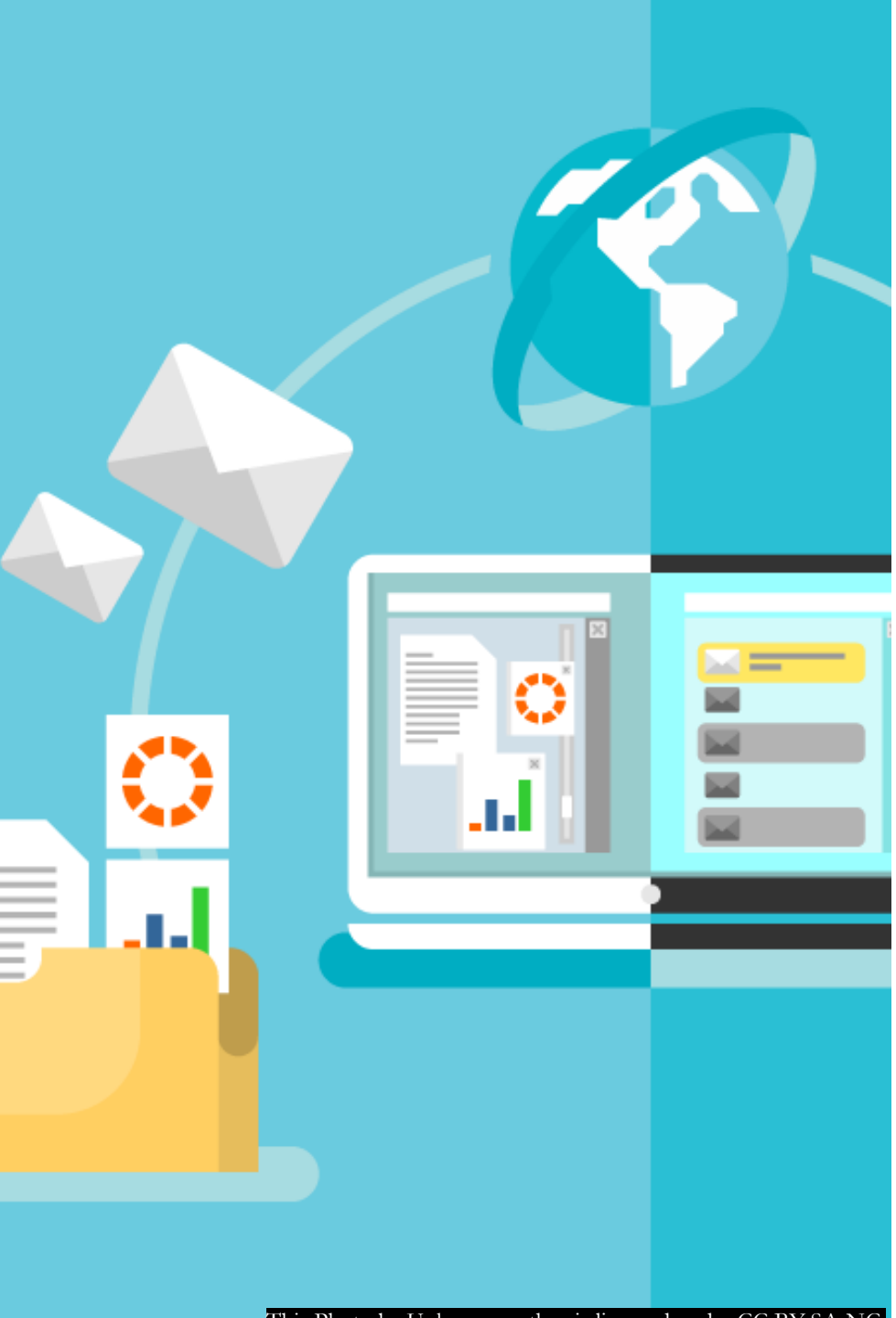
GDPR Data Transfers

(c) 2023 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown author is licensed under CC BY-SA.

How Do Diverging Privacy Standards Across Borders Cause Challenges with Data Transfers and Data Security?

(c) 2023 Lexeprint Inc. All Rights Reserved



GDPR Cross-Border Data Transfer

- Permits that transfers of personal data to countries outside the European Economic Area may take place if these countries have an "adequate level of data protection."
- Provides that the third countries' level of personal data protection is assessed by the European Commission, and the adequacy decision may be limited to more specific territories within a country (Article 45).

(c) 2023 Lexeprint Inc. All Rights Reserved.



Max Schrems v. Data Protection Commissioner (2020)

- **Ruling:** In August 2020, the Court of Justice of the European Union (CJEU) found that the EU-U.S. Privacy Shield was invalid and closed off key mechanisms for transferring persona data from the EU to the U.S.
- **Observations:**
  - This is the second time the CJEU has found the GDPR mechanisms for transferring personal data from the EU to the U.S. is invalid.
  - Significant impacts on trade and the development of technologies such as cloud computing and AI.

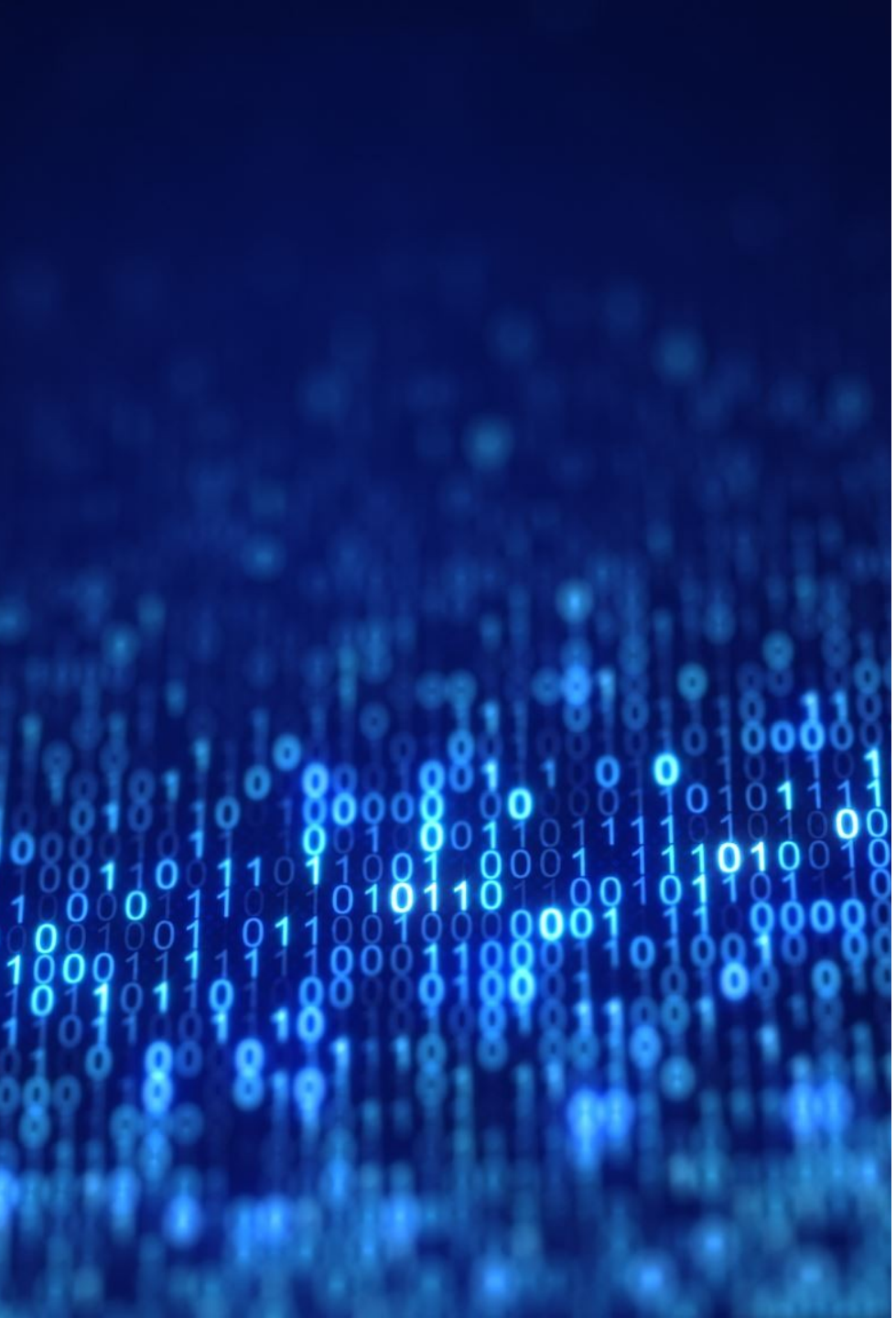
(c) 2023 Lexeprint Inc. All Rights Reserved.



Standard Contractual Clauses (SCCs)

- In June 2021, the European Commission introduced new standard contractual clauses (SCCs) for data transfers between EU and non-EU countries.
- These clauses enable data importers and exporters to satisfy Article 46 of the GDPR – Transfer subject to appropriate safeguard states.
  - These model clauses for data transfer agreements are required between data controllers and data processors; and cannot be modified.
  - The SCCs include for 4 modules based on the role and location of data exporters and importers.
- All agreements were required to be update to the 2021 clauses by December of 2022.

(c) 2023 Lexeprint Inc. All Rights Reserved.



EU-U.S. Data Privacy Framework

- The E.U. Data Privacy Framework is the successor to the Privacy Shield.
- In July of 2023, the DPF received adequacy approval from the European Commission, after it concluded that through this framework the US would ensure an adequate level of protection for the transfer of personal data, "comparable to that of the European Union."
- The DPF contains binding safeguards that address the concerns raised by the ECJ with the privacy shield, such as limiting US intelligence access to EU data.
- The DPF may still face legal challenges, as did the Privacy Shield.

**European Commission*

(c) 2023 Lexeprint Inc. All Rights Reserved.



GDPR Liability, Fines, and Class Actions

This Photo by Unknown author is licensed under CC BY-NC-ND.

(c) 2023 Lexeprint Inc. All Rights Reserved.

What is the Cost of Non-Compliance with the GDPR? Are Fines Sufficient Incentives?

(c) 2023 Lexeprint Inc. All Rights Reserved



What are the Consequences of Violating the GDPR Regulation?

- Fine of either €20 million or up to 4% of annual revenue (whichever is more) for:
  - Not having a "lawful basis" to process data or getting insufficient consent; or
  - Not being able to allow individuals to exercise their rights
- Fine of €10 million or up to 2% of annual revenue for:
  - Not having records in order; or
  - Not providing proper notification of a breach.*

* https://gdpr.eu/fines/

(c) 2023 Lexeprint Inc. All Rights Reserved.



GDPR Penalty Criteria

- Fines are administered by individual member state supervisory authorities and the following criteria are to be used to determine the amount of the fine on a non-compliant firm. These include:
  - **Nature of infringement**: number of people affected, damaged they suffered and duration of infringement.
  - **Intention**: whether the infringement is intentional or negligent.
  - **Mitigation**: actions taken to mitigate damage to data subjects.
  - **Preventative measures**: the extent of technical and organizational preventative action the firm has implemented.*

* Article 83.1, GDPR

(c) 2023 Lexeprint Inc. All Rights Reserved.



GDPR Penalty Criteria

- These also include:
  - **History**: past relevant infringements which may be interpreted to include infringements under the GDPR and Data Protection Directive (DPD).
  - **Cooperation**: firm's cooperation with the supervisory authority to remedy infringement.
  - **Data type**: what types of data the infringement impacts.
  - **Notification**: whether the infringement was proactively reported to the supervisory authority.
  - **Certification**: whether the firm had qualified under approved certifications or approved codes of conduct.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC

GDPR Fines to Date

- EU Data Protection authorities have handed out €4.05 billion in fines as of August 2023.
- In 2022, GDPR fines amounted to €830 million ($881 million), 80% of which was incurred by Meta Platforms, Inc.
- Notifications of data breaches increased by 8% to 365 a day on average.
- The most common types of fines are “insufficient legal basis for data processing” with 578 fines and "non-compliance with general data processing principles," with 469 fines.
- Spain has the highest number of GDPR fines by country, 717 fines in total.
- Ireland has imposed the highest total aggregate fines, € 2,510,343,400 from 26 fines.

**Enforcement Tracker*

(c) 2023 Lexeprint Inc. All Rights Reserved.



Austrian Post - €9.5 million ($10 million)

- In October 2019, the Austrian Data Protection Authority announced that it had enforced a fine on the country's postal service for illegally selling consumer data in violation of GDPR requirements.
- Investigators established that the Austrian Post had reviewed consumer information to determine whom would vote for which political party they may support and traded that data.
- Although it is not illegal under the GDPR, the Austrian Post was also found to have processed information on package frequency and the rate of relocations for direct marketing objectives.



Meta- €1.2 billion ($1.3 billion)

- The biggest GDPR fine in the regulation's history yet.
- In May 2023, Meta received a €1.2 billion fine from the Irish Data Protection Commission (DPC) for its data transfer mechanisms from the EU to the US.
- The DPC stated that Meta's Facebook's use of standard contractual clauses "did not address the risks to the fundamental rights and freedoms" of users following the 2020 ECJ decision invalidating the Privacy Shield.
- Along with the fine, the DPC issued an order for Facebook to suspend its future personal data transfers to the US within 5 months of the decision and establish compliant data flows.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Meta Platforms Ireland v. Federation of German Consumer Organisations (2022) CJEU

- **Facts:** In 2018, the Federation of German Consumer Organisations brought an action against Meta Platforms Ireland for its handling of user personal data with free games provided by third parties.
- **Issues:** Following the adoption of GDPR, do consumer protection associations still have a standing to autonomously bring civil proceedings against parties infringing the regulation?
- **Ruling:** In April 2022, the European Court of Justice ruled that "consumer associations may bring representative actions against infringements of personal data protection." It also noted that consumer protection associations fall within the scope of a "body that has standing to bring proceedings" for the GDPR public interest objective.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Meta Platforms Ireland v. Federation of German Consumer Organisations (2022) CJEU

- **Observations:**
  - In practice, consumer groups may autonomously bring opt-out class actions for alleged breaches of data protection rules.
  - The decisions lowers the threshold for consumer groups to make claims of consumer protection violations if the practices also involve data privacy and protection.
  - The court noted that the GDPR is a "harmonization of national legislation on the protection of personal data" but that it does leave additional discretion to Member States for complementary actions.

(c) 2023 Lexeprint Inc. All Rights Reserved.



(c) 2023 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Founder
JAMS – Neutral
Harvard – Faculty
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Shannon Yavorsky
Orrick, Herrington & Sutcliffe LLP – Partner
Contact:
E: syavorsky@orrick.com
URL: https://www.orrick.com/

Shannon Yavorsky is the head of Orrick's global Cyber, Privacy & Data Innovation group and a leading authority on United States (U.S.) and European (EU) privacy, cybersecurity and artificial intelligence (AI) issues. She is uniquely qualified in California, England and Wales and helps global companies navigate the increasingly complex global privacy, cybersecurity and artificial intelligence regulatory landscape.

She advises public and private companies across several sectors, including life sciences and health technology, financial services, private equity, insurance, social media and technology on a range of EU and U.S. federal and state privacy laws. Shannon's strategic counseling advice includes, but is not limited to:

- Advertising and payment card processing self-regulatory frameworks
- Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM)
- Electronic Communications Privacy Act (ECPA)
- EU Artificial Intelligence Act
- EU e-Privacy Directive
- EU General Data Protection Regulation (GDPR)
- Fair Credit Reporting Act (FCRA)
- Gramm–Leach–Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework
- Telephone Consumer Protection Act (TCPA)
- U.S. state breach notification laws
- U.S. state privacy laws in California, Colorado, Connecticut, Utah and Virginia (CCPA, CPRA, CPA, CTDPA, UCPA, VCDPA)

Shannon also helps clients undertake comprehensive privacy, cybersecurity and artificial intelligence risk assessments, evaluates privacy, security and artificial intelligence risks in corporate transactions and drafts and negotiates data-related contracts. She advises clients on cross-border data transfers, data breaches and developing global privacy and artificial intelligence compliance programs.

(c) 2023 Lexeprint Inc. All Rights Reserved.