2022 Year in Review: GDPR Enforcement and What Lies Ahead

Part 2 of 3

Speakers:

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

Shannon Yavorsky, Partner, Orrick, Herrington & Sutcliffe LLP

Ashley Winton, Partner, Mishcon de Reya LLP

Samantha Ettari, Senior Counsel, Perkins Coie, LLP

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.

Speakers

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

Shannon Yavorsky
Partner
Orrick, Herrington &
Sutcliffe LLP

Ashley Winton
Partner
Mishcon de Reya
LLP

Samantha Ettari
Senior Counsel
Perkins Coie LLP

Agenda

Part 1:

- Introduction to the General Data Protection Regulation (GDPR)
- The Principles of GDPR
- Data Subject Rights Under GDPR

Part 2:

- **GDPR Obligations for the Data Controller and Processor**
- **GDPR Data Transfers**
- **GDPR Enforcement**

Part 3:

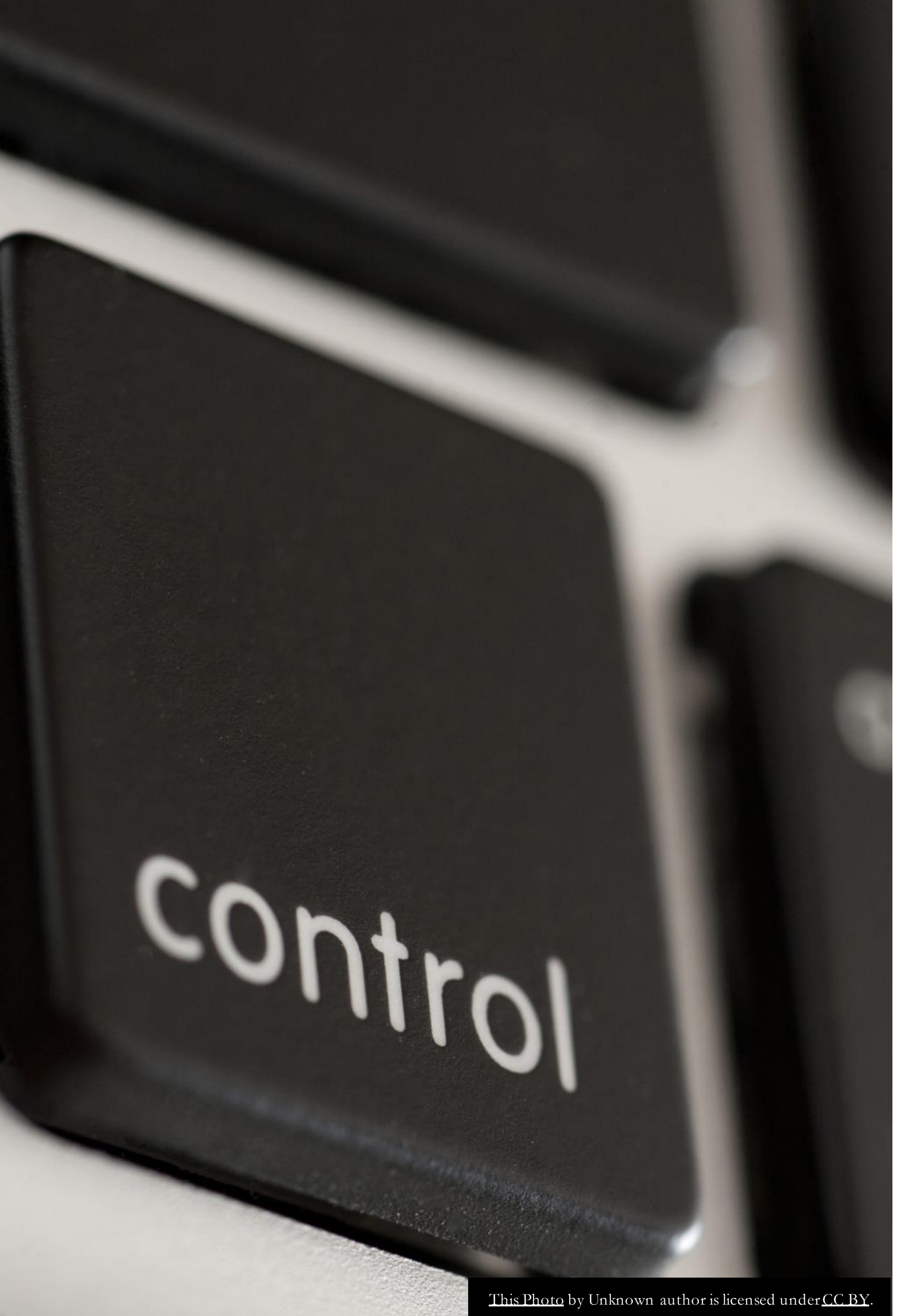
- GDPR Class Action Cases
- European Network and Information Security Agency (ENISA)

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

Review of 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 has a global reach, as its scope can be triggered by either or both location and the offering of "goods and services" in the EU.

GDPR Obligations for the Data Controller and Processor



This Photo by Unknown author is licensed under CC BY.

Data Controller

- The party that determines the purposes of any personal data and the means of processing it.

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.

Data Processors

- The party that processes personal data on behalf of a data controller.

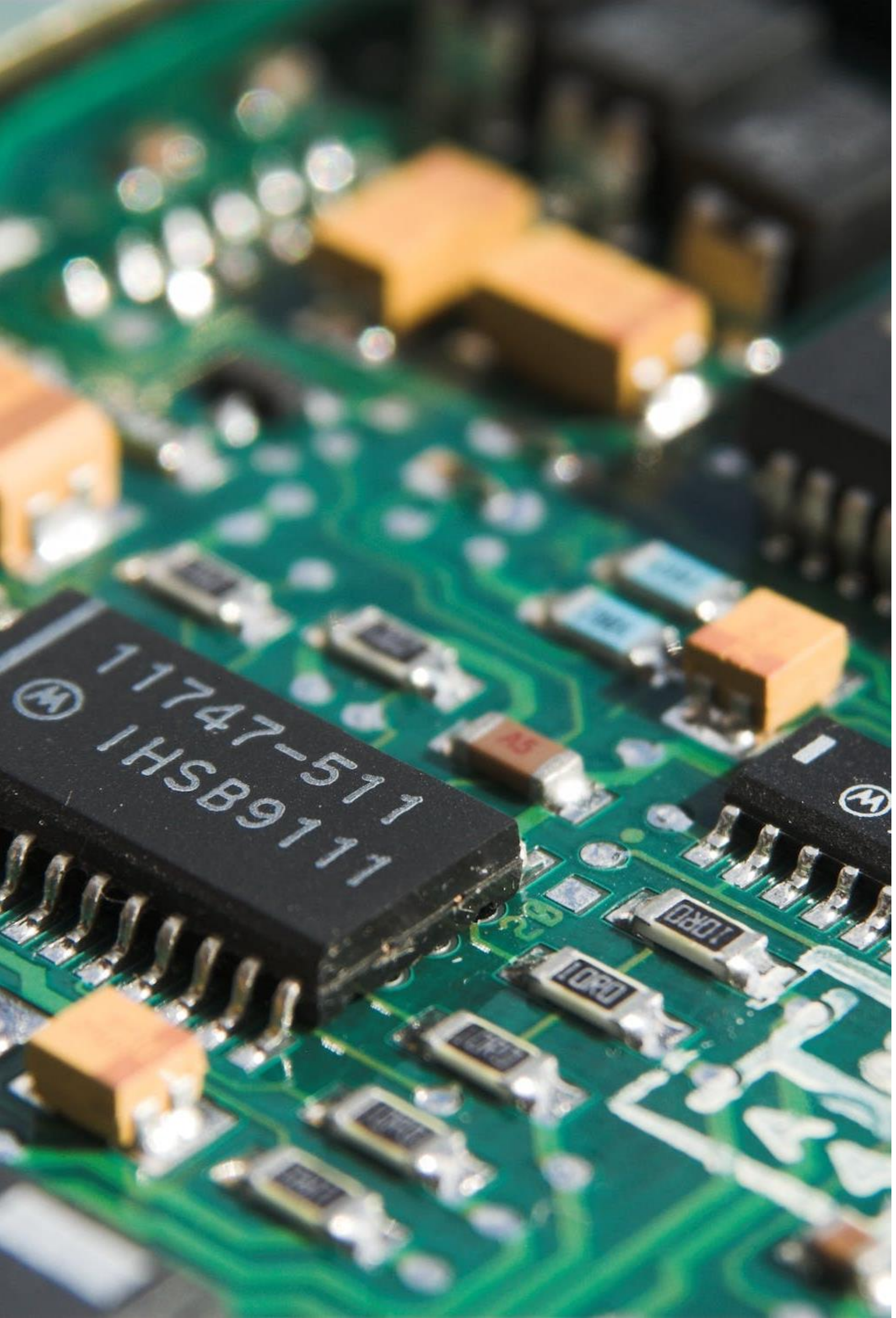
Obligations (GDPR Article 28)

- 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

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

Data Protection Officer

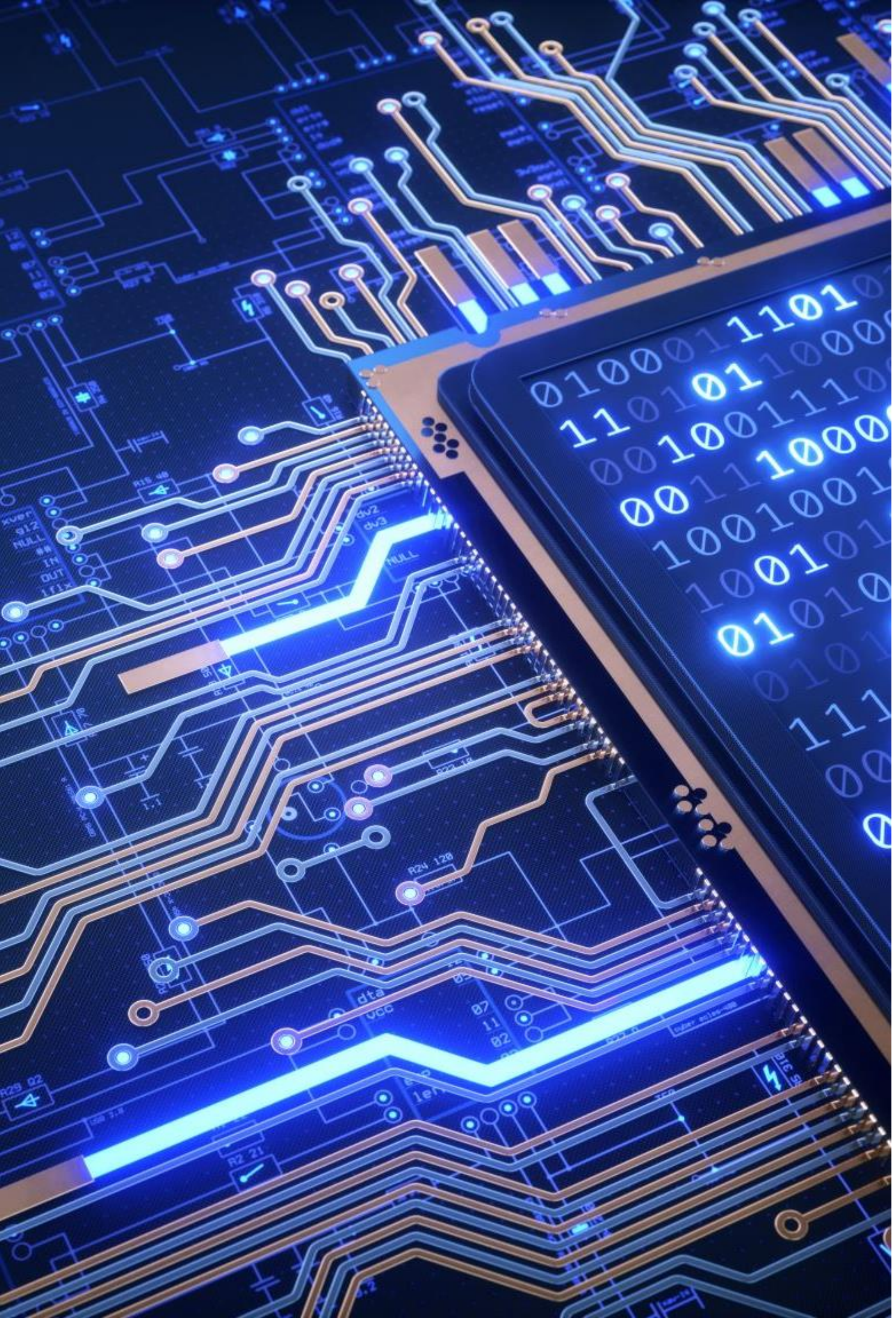
- What is a Data Protection Officer (DPO)?
  - A DPO must provide expert professional knowledge in data protection law and IT security (the scope depends on the complexity of data processing and the size of the company).
  - Relevant companies have two possibilities to meet their obligation to appoint a DPO: (1) to name an employee as an internal DPO or (2) to appoint an external DPO.



Data Protection Officer

- Who needs to appoint a DPO?
  - (1) Any data processor or controller whose processing is carried out by a public authority or body, except for judicial courts;
  - (2) Any data processor or controller whose core activities require regular and systematic monitoring of data subjects on a large scale; or
  - (3) Any data processor or controller whose operations involve the processing of special categories of data defined in Article 9 and Article 10. This includes data relating to criminal convictions, public health and specific historic or scientific research purposes.*

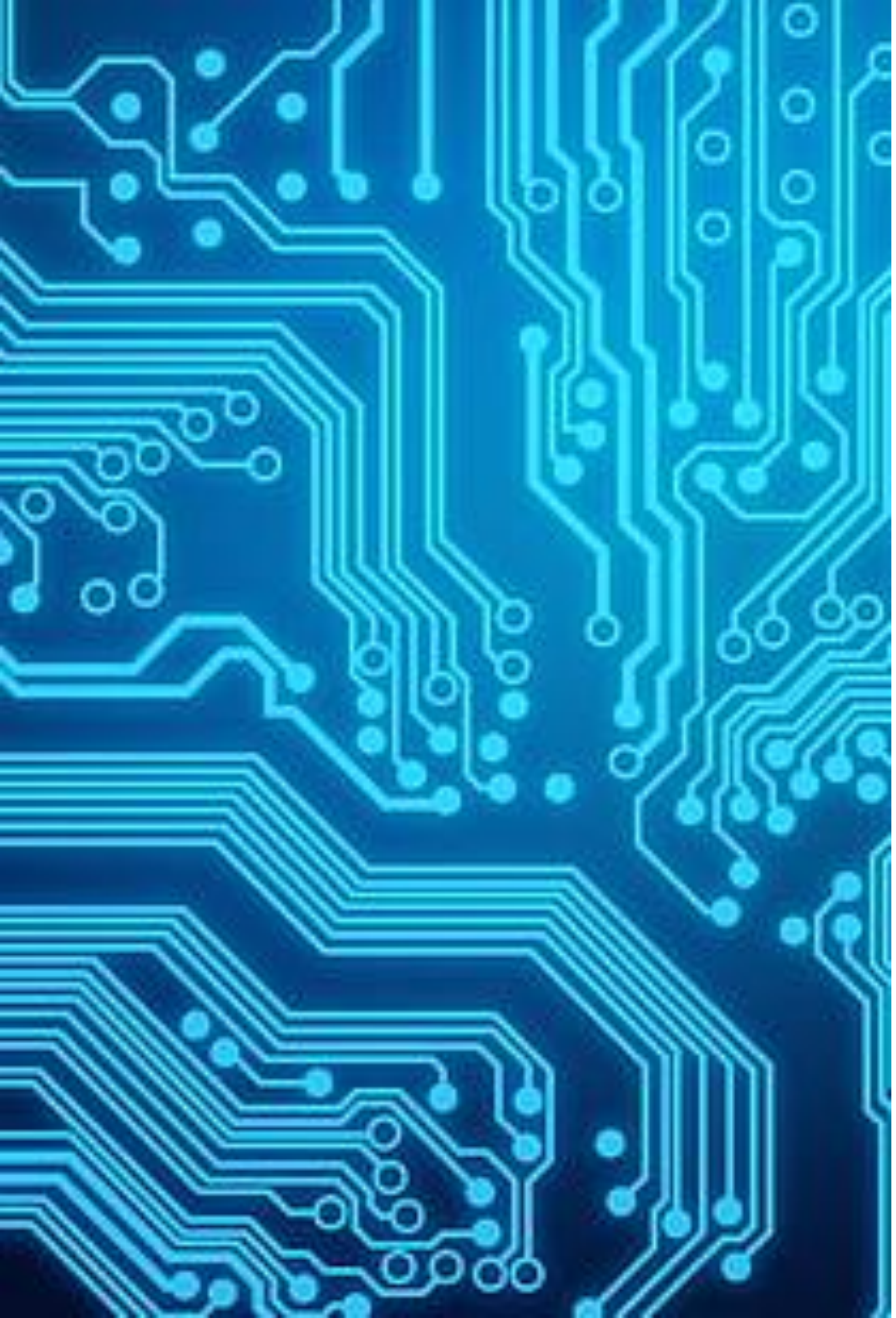
** Article 37, GDPR*



Data Protection Officer

- What are the duties of a Data Protection Officer?
  - (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.*

* *Article 37, GDPR*



Data Protection: Privacy by Design

- **Privacy by Design:** the GDPR outlines that 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.
- In terms of process implementation, the Regulation details utilizing best practices in data minimization, pseudonymization, and process documentation. *

** Article 25, GDPR*

Data Protection: Privacy by Default

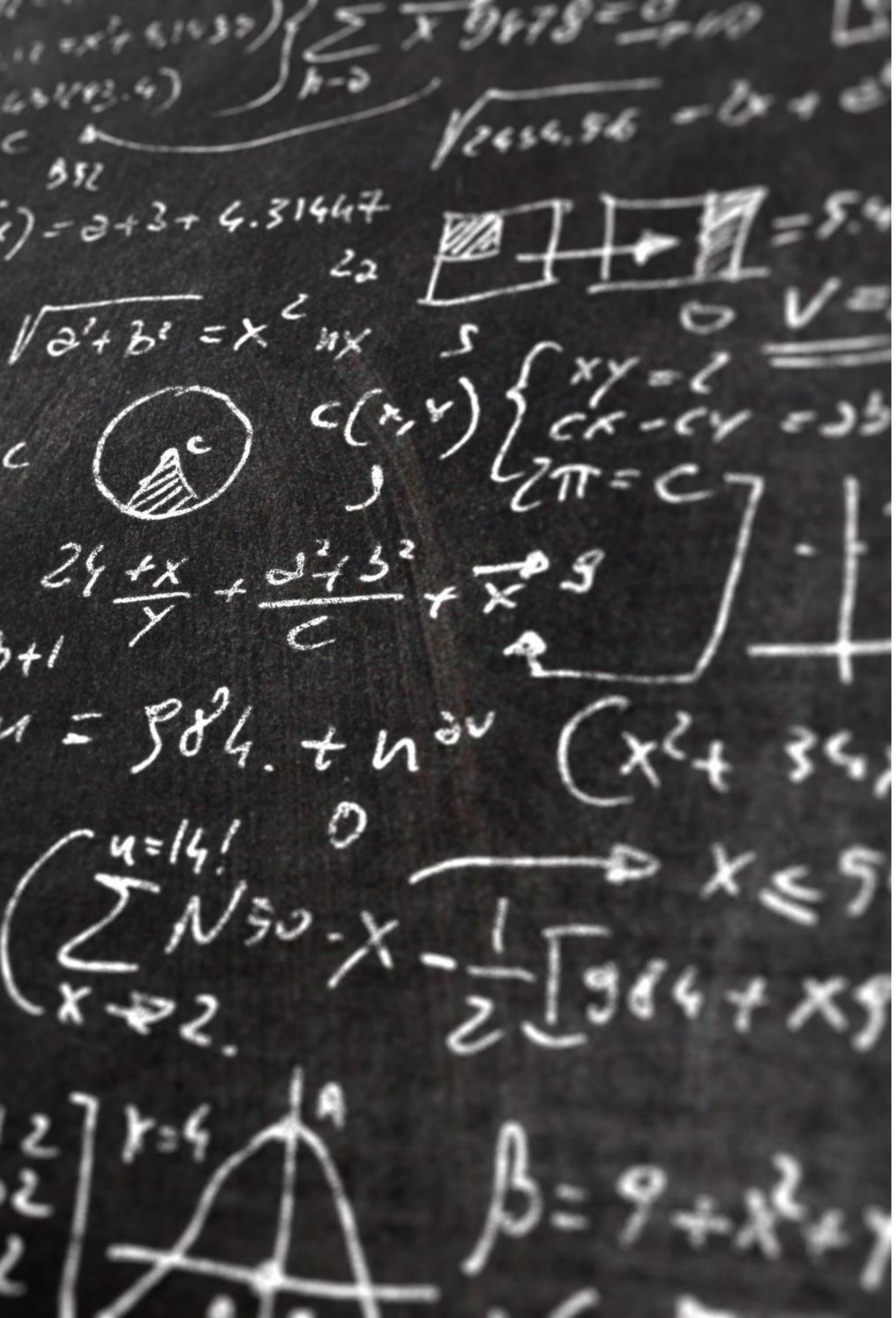
- **Privacy by Default:** entails taking data protection measures as the rule, not the exception. As such, the GDPR states that measures must be taken by default to ensure that only the personal data necessary for each specific business purpose is processed.
- In practice, companies must have a well-defined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

* *Article 25, GDPR*

Data Protection Impact Assessment (DPIA)

- A Data Protection Impact Assessment (DPIA) is 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.*
  - The DPIA is a DPO responsibility.
- Examples of the types of conditions that would require a DPIA:
  - Processing children's data;
  - Using new technologies;
  - Tracking people's location or behavior; and
  - Processing personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs.

** Article 35, GDPR*



What does a Data Protection Impact Assessment need to 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.*

* Article 35, GDPR

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

Data Processing Agreement Requirements

- A Data Processor Must:
  - Agree to process personal data only written by the instructions of the controller;
  - Not hire another processor unless instructed;
  - Support the controller with upholding GDPR obligations;
  - Ensure confidentiality for everyone who interacts with the data;
  - Agree to delete personal data or return it to controller after termination of services;
  - Allow controller audits and will provide all necessary information for compliance;
  - Use appropriate technical and organizational measures to protect the security of the data; and
  - Compensate potential breach of contract.*

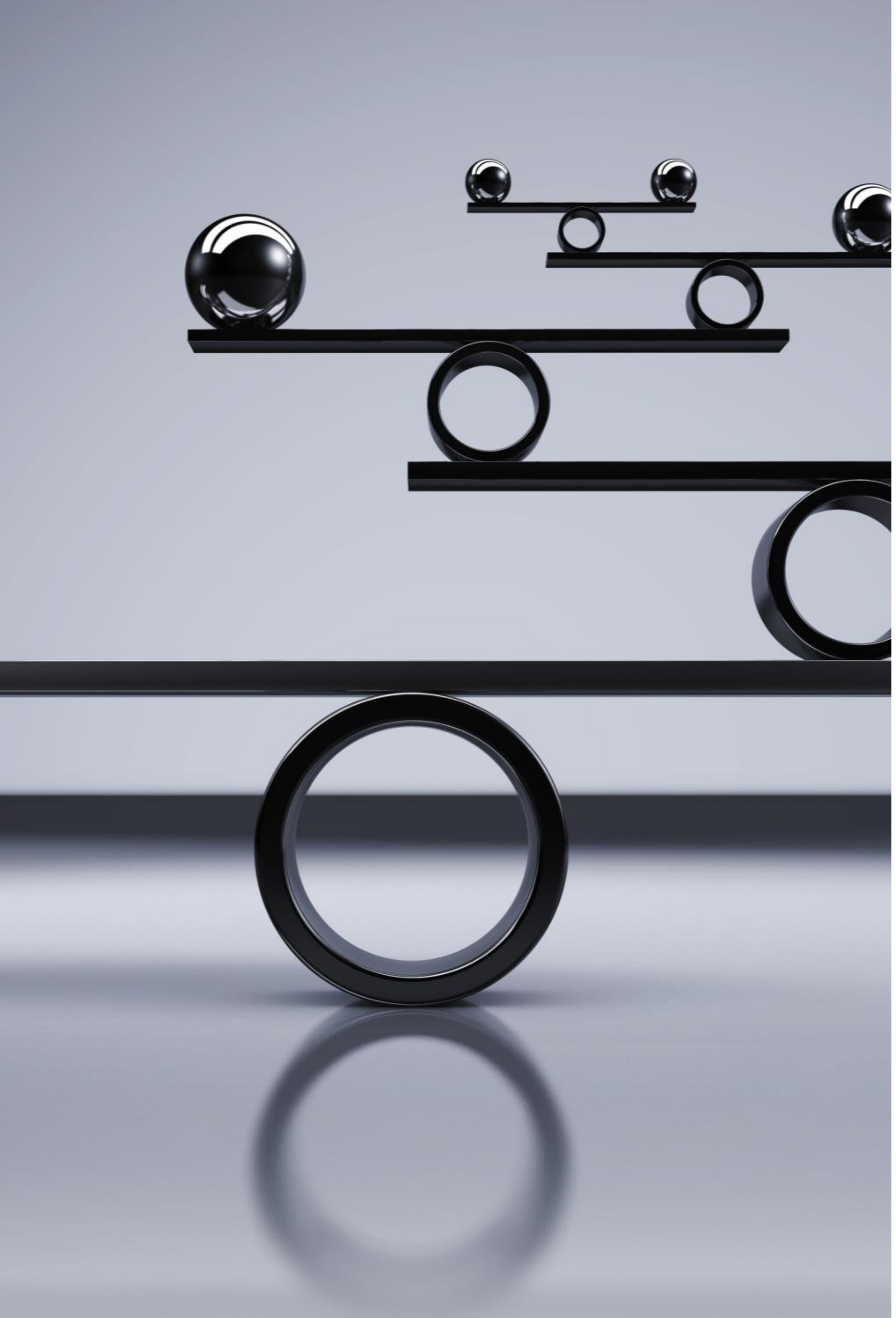
* Article 28, GDPR

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. The data subject gave specific, **unambiguous consent** to process the data. (e.g., They've opted into a marketing email list).
2. Processing is necessary to execute or to prepare **to enter into a contract** to which the data subject is a party.
3. Data processing is necessary **to comply with a legal obligation.***

* Article 6, GDPR



What are the Legal Bases for Data Processing? (cont.)

4. Data processing is necessary **to save somebody's life**.

5. Data processing is necessary to perform a task in the **public interest** or to carry out some official function (e.g., the company is a private garbage collection company).

6. Data collector has a **legitimate interest** to process someone's personal data. Though this condition is flexible, the fundamental rights and freedoms of the data subject always override this interest.*

* Article 6, GDPR

The Importance of Consent

- The GDPR lists strict guidelines about what constitutes consent from a data subject to process their information, including:
  - Consent must be "freely given, specific, informed and unambiguous;"
  - Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language;"
  - Data subjects can withdraw previously given consent whenever they want;
  - Children under 13 can only give consent with permission from their parent; and
  - The data processor must keep documentary evidence of consent.*

* Article 7, GDPR

GDPR Data Transfers

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).

Max Schrems v. Data Protection Commissioner (2020)

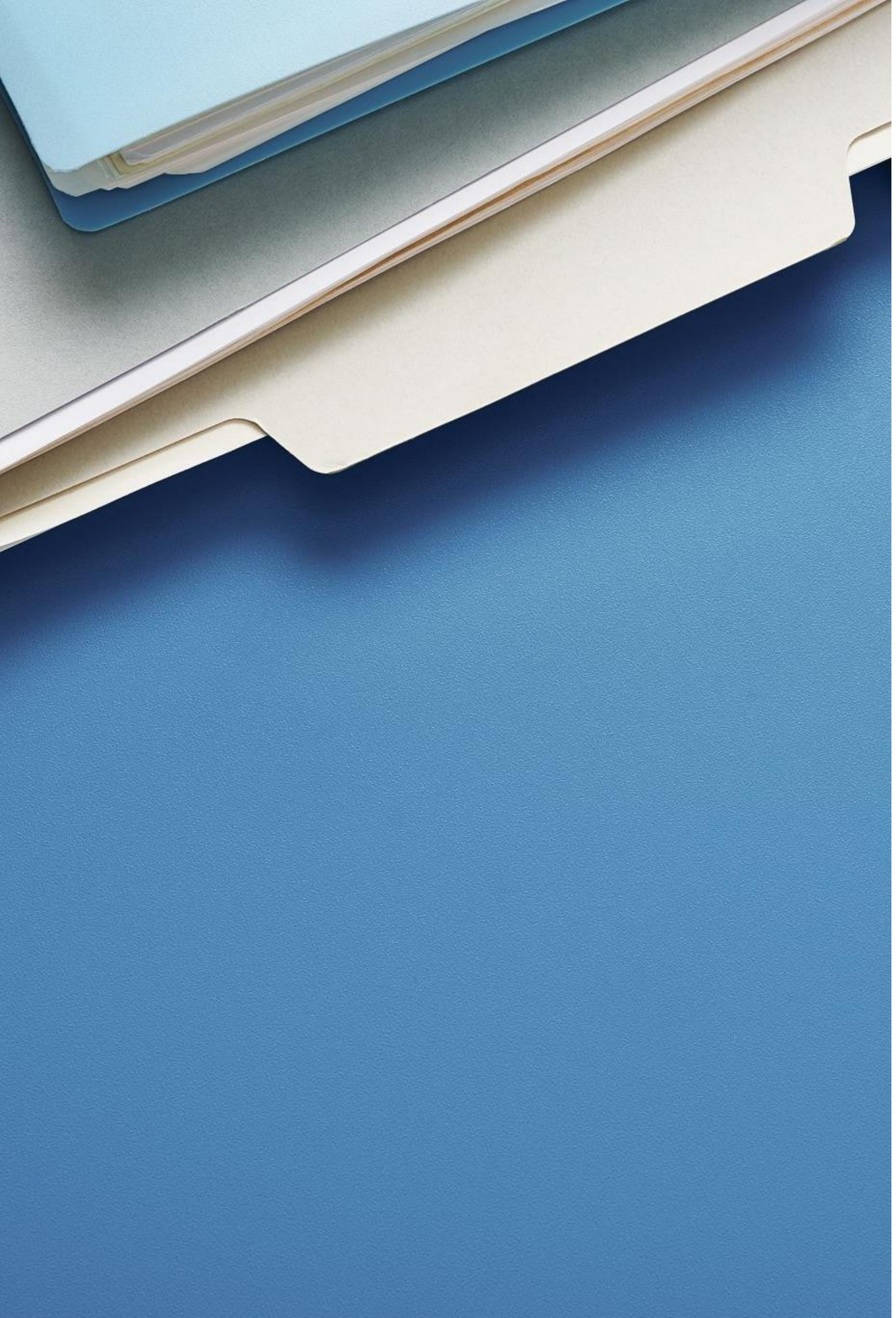
- **Ruling:** In August 2020, the Court of Justice of the European Union (CJEU) found that the EU-U.S. Privacy Shield was invalid and closed off key mechanisms for transferring persona data from the EU to the U.S.
- **Observations:**
  - This is the second time the CJEU has found the GDPR mechanisms 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.

This Photo by Unknown author is licensed under CC BY.

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.

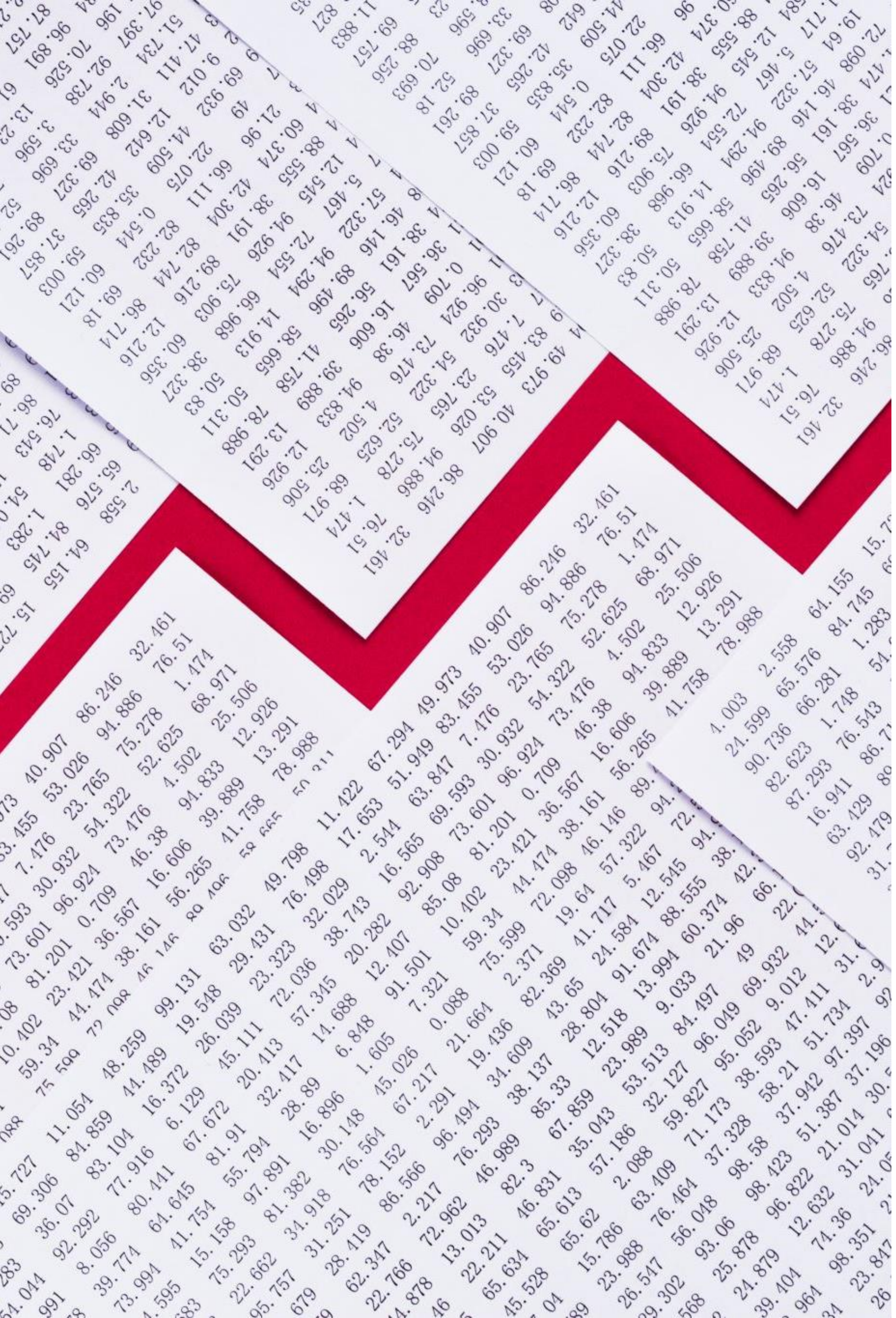
GDPR Enforcement



What are the Consequences of Violating the GDPR Regulation?

- Fine of either €20 million or 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 2% of annual revenue for:
  - Not having records in order; or
  - Not providing proper notification of a breach.*

* https://gdpr.eu/fines/



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.*

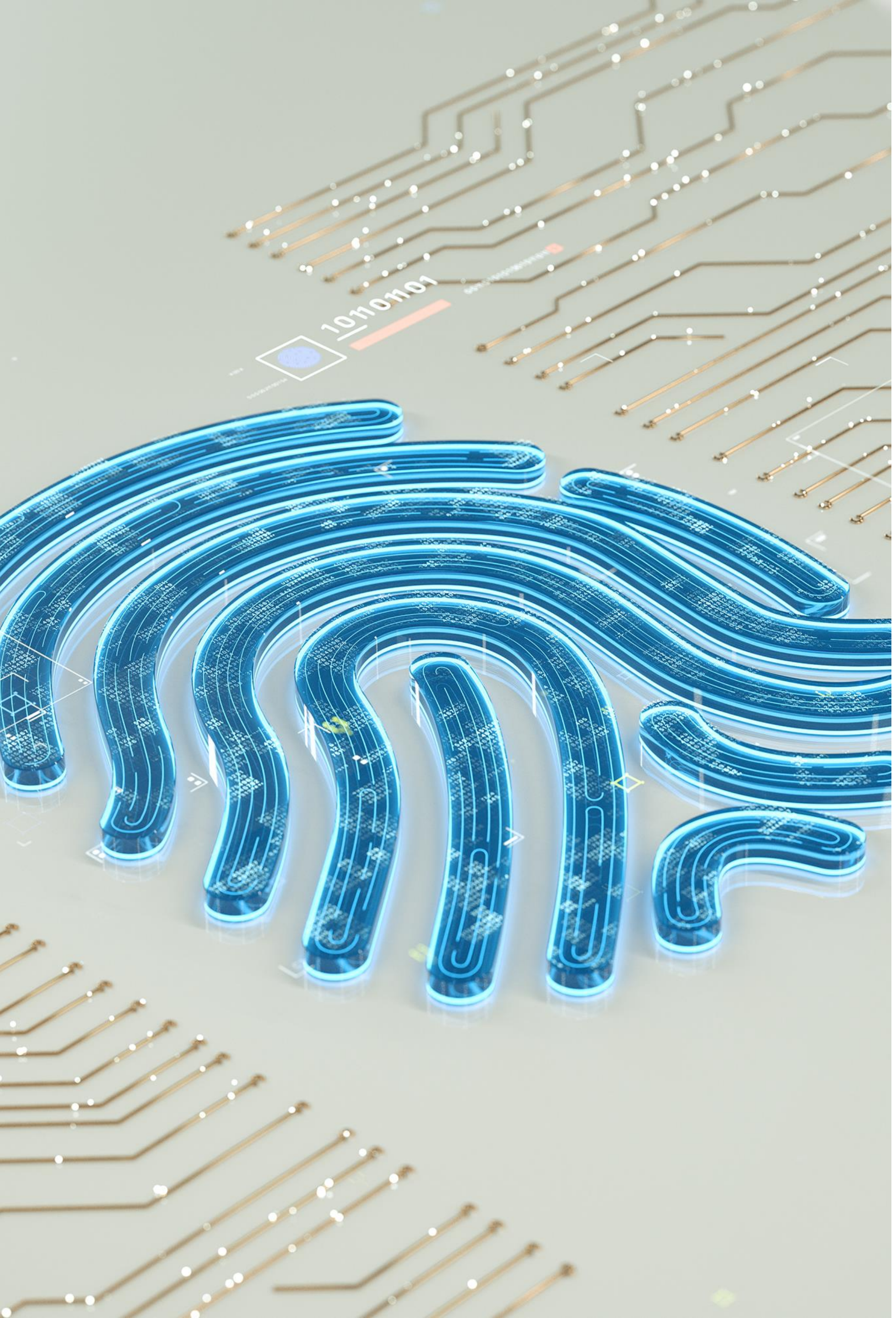
* Article 83.1, GDPR

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.

GDPR Fines to Date

- The highest GDPR fine between May 2018 and January 2023 was imposed by Luxembourg to Amazon for a total of €746 million.
- Spain has the highest number of GDPR fines by country, 572 fines in total.
- Ireland has imposed the highest total aggregate fines, € 1,309,115,900 from 21 fines.



GDPR Fines to Date

- EU Data Protection authorities had handed out €2.34 billion in fines as of January 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 "non-compliance with general data processing principles," with 363 fines, and "insufficient legal basis for data processing" with 476 fines.

**Enforcement Tracker*

Amazon - €746 million ($888 million)

- The biggest GDPR fine in the regulation's history.
- In July 2021, Luxembourg's data protection authority fined Amazon €746 million following an investigation into the company's processing of customer data.
- Amazon spokesperson strongly disagreed, stating that "the decision relating to how we show customers relevant advertising relies on subjective and untested interpretations of European privacy law".

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

Meta, Inc. - €390 million ($410 million)

- Meta reigned in 2023 by receiving fines to both Facebook and Instagram from the Irish Data Protection Commission (DPC).
- This sanction came after Meta received the second largest GDPR fine in the regulation's history in 2022 for its processing of child user data on Instagram, €405 million.
- These fines represented the final decisions of two long-running inquiries confirming that contractual obligation is not appropriate justification for processing personal data for behavioral ads.
- The fines were accompanied by corrective measures which order Meta to be GDPR compliant within 3 months.

This Photo by Unknown Author is licensed under CC BY-NC

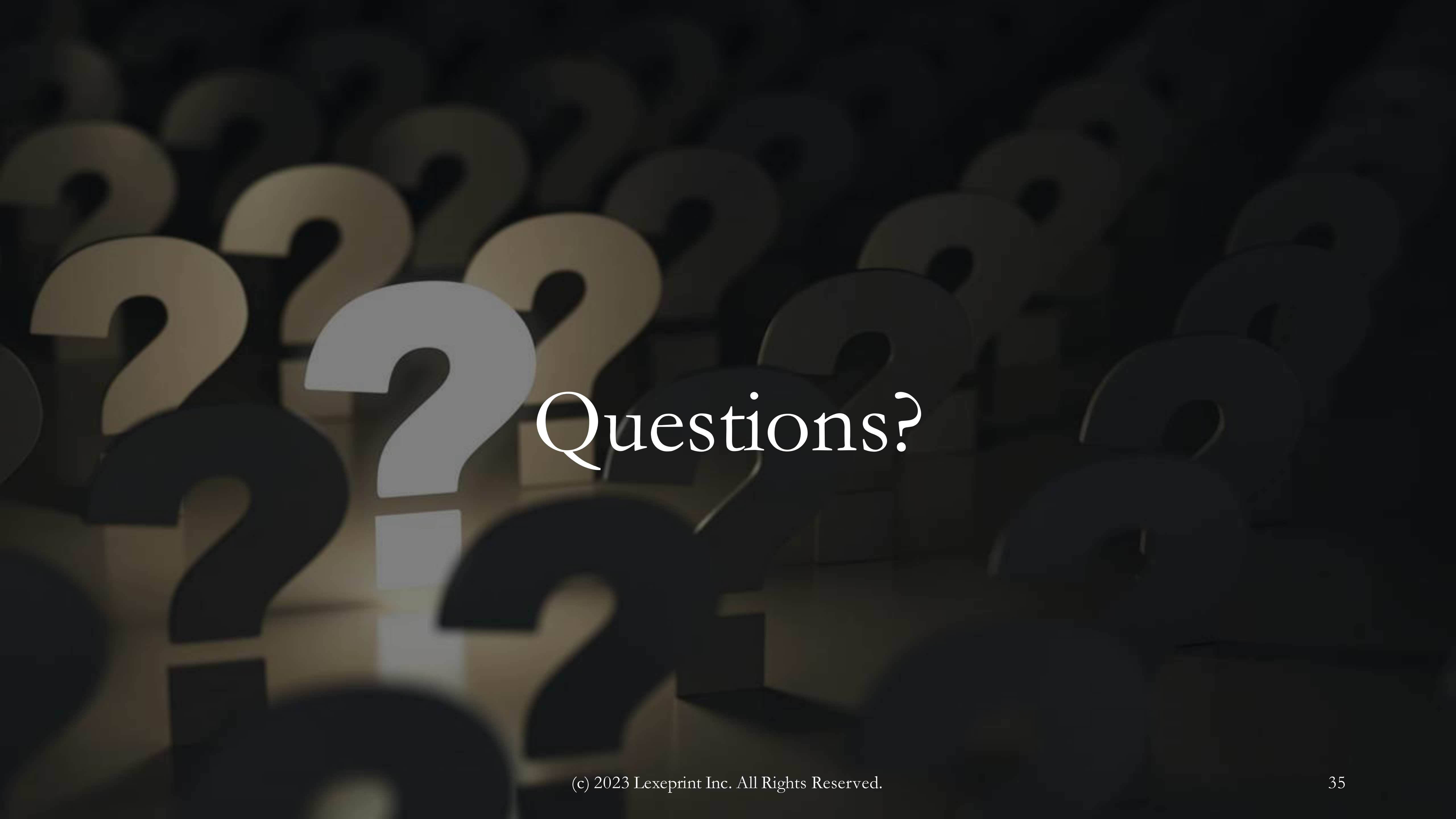
WhatsApp - €225 million ($236 million)

- In September 2021, the Irish Data Protection Commissioner concluded a three-year investigation into WhatsApp and concluded that the company failed to fully disclose to European users how it used their data.
- Specificity of the issue laid in WhatsApp sharing of data with Facebook (Meta).
- Similar to Amazon, a WhatsApp spokesperson said the company strongly disagreed with the decision and would appeal.

This Photo by Unknown author is licensed under CC BY.

REWE International - €20 million ($26 million)

- GDPR regulatory enforcement does not only target software or web-based companies. British Airways, Amazon Road Transport, H&M, and the Austrian Post have all been fined in the last few years.
- In 2022, Rewe International, an Austrian supermarket and drugstore company, was fined €8 million for its handling of customer data in its customer loyalty and rewards program, which collected and used user data without consent.



Questions?

Contact Us

Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com

Samantha Ettari
Email: SEttari@perkinscoie.com
URL: https://www.perkinscoie.com/en/

Shannon Yavorsky
Email: syavorsky@orrick.com
URL: https://www.orrick.com/

Ashley Winton
Email: ashley.winton@mishcon.com
URL: https://www.mishcon.com

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.

Shannon Yavorsky
Orrick, Herrington & Sutcliffe LLP – Partner
Contact:
W: (415) 773-5731
E: syavorsky@orrick.com
URL: https://www.orrick.com/

Shannon K. Yavorsky is a leading authority on U.S. and European data privacy and security issues. She is uniquely qualified in California, England and Wales and Ireland, bringing a deep understanding of the increasingly complex global privacy and data security regulatory landscape.

Shannon routinely advises clients on a broad range of U.S. and European data privacy and cybersecurity issues. She advises on emerging issues surrounding the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR) and the e-Privacy Directive. Shannon helps clients undertake comprehensive privacy and cybersecurity assessments worldwide, evaluate privacy and security risks in corporate transactions, and draft and negotiate contracts concerning data-related vendors and arrangements. She also advises and represents clients on cross-border data transfers, data breaches and developing global privacy compliance programs. She has significant experience with model contract clauses, privacy policies, website terms and conditions, data processing agreements, and self-certifying to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

In addition to the GDPR and CCPA, Shannon advises on an array of privacy and security laws and regulations, including the FCRA, ECPA, TCPA, HIPAA, CAN-SPAM, GLBA, state breach notification laws, and self-regulatory frameworks, including those covering online advertising and payment card processing.

Shannon's clients are multinational clients across diverse industry sectors, with an emphasis on technology, financial services, retail, staffing, advertising, healthcare, and automotive.

Ashley Winton
Mishcon de Reya LLP – Partner
Contact:
E: ashley.winton@mishcon.com
W: +44 20 7577 6950
URL: https://www.mishcon.com/

Mishcon de Reya

Ashley Winton focuses his practice on global data protection and privacy, information governance and cybersecurity compliance. He has particularly in-depth knowledge of cyber breach response, cybersecurity in the context of payment systems, the lawful interception of data, and the conflict of laws in relation to corporate and government investigations and international litigation. Ashley frequently represents major corporations, trade associations, charities and government entities on a range of data privacy and cybersecurity issues and he has significant experience in advising on the impact of privacy and cybersecurity law on cloud services, health care and international data transfers.

Ashley is a fellow of the Ponemon Institute and current Chairman of the Data Protection Forum, the leading data protection association in the UK.

Recognitions

- Chambers & Partners UK 2020, UK Data Protection & Information Law, listed annually since 2001
- Chambers & Partners UK 2020, Information Technology, listed annually since 2001
- Legal 500 UK 2018, Data Protection, listed annually since 2001

Samantha Ettari
Perkins Coie LLP – Senior Counsel
Contact:
E: SEttari@perkinscoie.com
W: (214) 965-7700
URL: https://www.perkinscoie.com/en/

PERKINS COIE
COUNSEL TO GREAT COMPANIES

Samantha Ettari counsels clients on privacy, data security, and data management. She has significant experience with legal, practical, and reputational risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. She advises clients on both domestic and international privacy statutes and regulations, as well as cross-border transfers of data. Ms. Ettari represents clients in data access, data sharing, data transfers, and vendor management matters, as well as data breach management, readiness, and prevention, incident response, law enforcement coordination, and post-breach recovery. She assists clients in drafting and implementing global privacy policies, terms of use, data retention policies, information security procedures, and incident response and breach communication plans.

Ms. Ettari has an extensive and diverse background in commercial litigation, including complex contract and licensing disputes, advertising litigation, business torts, consumer fraud defense securities suits, and regulatory investigations defense—all of which she brings to her privacy and data security work. She has first- and second-chaired numerous federal and state trials and hearings, as well as domestic and international arbitrations. Her cybersecurity experience includes working with clients in the aftermath of security incidents and man-in-the-middle attacks, helping clients establish robust privacy programs, and advising on vendor and licensing agreements that contemplate the transfer and security of data. She has advised leading private equity firms, SaaS service providers, and e-commerce clients on privacy and data security issues in technology-driven acquisitions.

As a seasoned litigator, Ms. Ettari also has significant experience guiding clients through their obligations in the rapidly evolving area of electronic discovery, including implementing timely legal holds, minimizing spoliation, preserving and collecting evidence, and establishing and complying with information governance and email, text, and social media use policies.

Sam is a Certified Information Privacy Professional for the European Union (CIPP/E) and for the United States (CIPP/U) and a Certified Information Privacy Manager (CIPM). Prior to her relocation to Dallas, she served as co-chair of the New York State Bar Association Commercial and Federal Litigation Section's committees on privacy, data security, and information technology litigation. Ms. Ettari has been quoted in the *Wall Street Journal* and the *New York Times* on workplace privacy and geolocation tracking, and is a prolific writer on international and domestic privacy and data security law developments.