



Introduction to EU General Data Protection Regulation: Planning, Implementation, and Compliance

Gabriel Buehler
Priscilla Chataika
Julian Schneider
Alex Sharpe

CYBER SECURITY & DATA PRIVACY 2024



Practical & Entertaining Education for:

- Attorneys • Accountants
- Business Owners
- Executives • Investors

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

Thank You To Our Sponsor...



Restructuring & Insolvency Professionals • Bankruptcy Trustees
• Chapter 11 Debtors • Assignees • Receivers • Article 9 Sellers

A Better Way to Conduct Single Asset Sales Online!

DailyDAC™ is excited to announce its partnership with [maxXasset™](#), a simpler, easier & better way to conduct asset sales.

Take charge of your sales process! Choose the auction date, set the terms, & establish the closing timeline to suit your needs. Create & upload relevant sale documents behind confidentiality agreements, review every bidder's credentials, decide whether to approve or deny them, & monitor the bidding in real time.

No need to schedule a zoom or have the sale in an office. Now, interested parties can bid anytime, from anywhere! [maxXasset™](#) is also perfect to use in conjunction with real-time auctions, with use cases that include using it as a tool to select a stalking horse or as a tool for a first & or second round in a two-round process.

Disclaimer

- The material in this webinar is for informational purposes only. It should not be considered legal, financial, or other professional advice.
 - You should consult with an attorney & another appropriate professional to determine what may be best for the needs of your specific situation.
 - While the webinar producers & speakers take reasonable steps to ensure that the information presented is accurate, they make no guarantee in this (or any) regard.

*** This PowerPoint was produced in connection with a video webinar that premiered on 10/9/25. If you are reading this without the benefit of having attended, then you are missing its real value. You can access the webinar on-demand at [West Legal Ed Center](#) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

Meet the Faculty

Panelists

[Gabriel Buehler](#) - Buehler Law, PLLC

[Julian Schneider](#) - University of California

[Alex Sharpe](#) - Sharpe Management Consulting LLC

Moderator

Priscilla Chataika - DailyDAC

About This Webinar

Introduction to EU General Data Protection Regulation: Planning, Implementation, and Compliance

- The GDPR changed the way the world collects, stores, and sends personal data. The GDPR is a broad EU regulation that requires businesses to protect the personal data of EU citizens, whether the business itself is in the EU or elsewhere.
- Since its implementation in 2018, companies that collect data on EU citizens must comply with strict rules for the protection of personal data or face heavy fines for non-compliance.
- This webinar will provide an overview of GDPR's applicability and requirements, as well as how your organization may meet those standards

About This Series

Cybersecurity & Data Privacy

- Cybersecurity and data privacy are critical topics of concern for every business in today's environment. Data breaches are a threat to every business and can cause both direct losses from business interruption and loss of data to indirect losses from unwanted publicity and damage to your business's reputation. Compliance with a patchwork of potentially applicable state and federal laws and regulations may cost your business in terms of money and time.
- This series discusses the various laws and regulations that affect businesses in the United States and in Europe, as well as the best practices to use in creating an information security program and preparing for and responding to data breaches.

Episodes In This Series

#1 Introduction to US Privacy and Data Security: Regulations and Requirements

Premiere date: 9/4/25

#2 Introduction to EU General Data Protection Regulation: Planning, Implementation, and Compliance

Premiere date: 10/9/25

#3 How to Build and Implement your Company's Information Security Program

Premiere date: 11/13/25

#4 Data Breach Response: Before and After the Breach

Premiere date: 12/11/25

Episode #2: Introduction to EU General Data Protection Regulation: Planning, Implementation, and Compliance

Each Financial Poise Webinar is delivered in Plain English, understandable to investors, business owners, & executives without much background in these areas, yet is of primary value to attorneys, accountants, & other seasoned professionals. Each episode brings you into engaging, sometimes humorous, conversations designed to entertain as it teaches. Each episode in the series is designed to be viewed independently of the other episodes so that participants will enhance their knowledge of this area whether they attend one, some, or all episodes.

Introduction

The General Data Protection Regulation (GDPR) is a law that regulates data protection for individuals in the European Union

- Passed by the EU Parliament in April 2016
- Enacted into law on May 25, 2018
- Most impactful data privacy legislation in 20 years
- Paved the way for similar legislation across the globe

Introduction *(cont'd)*

- Aims to protect EU citizens against privacy and data breaches; and
- Simplify regulations for international business by unifying data protection regulation in the EU into one law
- Enacted in response to a growing wave of global cyberattacks, data leaks, identity thefts
- Introduced to replace outdated data protection laws enacted during the infancy of the internet

Data Protection Laws Around the World following GDPR

- Brazil
- Australia
- Canada
- China
- California Consumer Protection Act and California Privacy Rights Act
- Japan
- South Korea
- Being compliant with GDPR does not mean you are compliant with all data protection laws

Important Metrics

- About 144 countries have privacy laws (iapp.org)
- The U.S. has one of the most fragmented privacy landscapes in the world. Instead of one comprehensive federal law like the GDPR, it relies on a patchwork of sector-specific federal rules — such as HIPAA for health and GLBA for financial data — alongside state-level legislation.
- As of 2025, around 20 states have enacted their own comprehensive consumer privacy laws, and every state has at least a data breach notification law. This creates a highly complex and sometimes inconsistent regulatory environment for businesses operating across the country.
- 6.6 billion people or 82% of the world's population is covered by some form of national data privacy law (iapp.org)

EU Data Privacy Regulation History – The “Directive”

1995 – EU adopts the European Data Protection Directive (95/46/EC)

- regulated both automated and manual processing of personal data adopted in response to European Convention of Human Rights (ECHR) Article 8 -
- which stresses that all humans have a right to privacy in their home and correspondence

EU Data Privacy Regulation History – The “Directive” *(cont’d)*

The Directive required data processing companies to comply with 3 principles when processing personal data -

- transparency
- legitimate purpose
- proportionality

GDPR Explained

- Gives consumers more control over how their data is collected and used
- Forces companies to justify what they do with personal information they collect, defined as any information that is identifiable to a specific person, such as:
 - ☐ Name
 - ☐ phone number
 - ☐ Username
 - ☐ health data
 - ☐ political opinions
 - ☐ IP address
 - ☐ location data
- Generally imposes responsibility and accountability on data collection and processing companies

GDPR Key Players

- Data subject: individual whose data is being processed
 - All natural persons who can be distinguished as persons with rights in regards to the processing of personal data
- Data controller: person/entity in charge of data processing
 - ☐ Natural person
 - ☐ Public authority or agency
 - ☐ Corporate entity

GDPR Key Players *(cont'd)*

- Data processors: processes data on behalf of the controller
 - ☐ Natural person
 - ☐ Public authority or agency
 - ☐ Corporate entity (such as a vendor)
- Data Protection Officer (DPO): compliance officer that helps ensure that an organization processes personal data in compliance with the law
- Example - an e-commerce business outsourcing analytics or a hospital and a hospital and a cloud provider

GDPR Requirements

- Article 5 of the GDPR sets out seven key principles:
 1. Lawfulness, fairness and transparency
 2. Purpose limitation
 3. Data minimisation
 4. Accuracy
 5. Storage limitation
 6. Integrity and confidentiality (security)
 7. Accountability

- These principles should lie at the heart of your approach to processing personal data.

Increased Territorial Scope

- GDPR abandons previous ambiguous language and replaces it with “clear guidelines”
 - Applies to the processing of personal data by controllers and processors in the EU- regardless of where the processing takes place; and
 - Data processing where the activities relate to offering goods or services to data subjects and the monitoring of behavior that takes place within the EU
- ✓ **Non-EU businesses engaged in processing the data of EU citizens must appoint a representative in the EU**

Article 6 of the GDPR

The lawful bases for processing are set out in Article 6 of the GDPR. Before any organization processes personal data, it must ensure that at least one of these legal grounds applies:

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (but this doesn't include obligations that come from a contract).
- (d) Vital interests: the processing is necessary to protect someone's vital interests.
- (e) Public task: the processing is necessary for you to perform a task in the public interest.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Lawful basis for processing personal data (Article 6)

- Requires companies to request and obtain consent from data subjects by *clear and plain* language (“opt-in consent”)
 - All requests must be given and written in an intelligible and easily accessible form and distinguishable from all other matters
- It must be just as easy to withdraw consent as it is to give it

Right to Access Article 15 of the GDPR

- Data subjects have the right to obtain confirmation from a controller as to whether or not their personal data is being processed, where its being processed, and for what purpose
 - If a request is made by the data subject, the controller must give the data subject a free electronic copy of his/her information

Right to be Forgotten Article 17 of the GDPR

- Data subjects may request to have controller –
 - erase personal data
 - cease further circulation of the data; and
 - potentially have third parties stop processing the data
- Individuals may request the deletion of their personal data if the data is no longer relevant to the original purpose or processing, or data subject is withdrawing consent, the data was unlawfully processed, or there's a legal obligation to erase it
- Erasure requests are weighed against the public interest in the availability of the data and data retention requirements

Data Portability

- Data subjects have the right to receive their personal data and may transmit such data to another controller as they please
- The data subject must be able to use the data when given by the data controller – must be given “in a structure, commonly used and machine-readable format”

Privacy-by-Design - reflected in GDPR Article 25's “data protection by design and by default”

- 7 Foundational (guiding) Principles common to Privacy Laws and Regulations.
 1. Proactive not reactive: anticipate and prevent privacy issues before they occur
 2. Privacy as default setting: personal data should be automatically protected without requiring user action
 3. Privacy embedded into design: integrate safeguards directly into your systems and workflows
 4. Full Functionality: balance all objectives, privacy doesn't have to come at the expense of innovation
 5. End to end security: ensure protection throughout the entire data lifecycle
 6. Visibility and transparency: keep data practices open and accountable
 7. Respect for user privacy: keep the user's interests front and center in all decisions
- Data protection is at forefront of any controller or processor system design - not an additional option or afterthought. It entails building privacy and data protection into systems and processes from the very beginning.
- Requires controllers hold and process only data absolutely necessary for completion of their duties, process it responsibly, and limit access to personal data

Data Protection Officer (DPOs)

- DPO appointment is mandatory only to companies (controllers) whose core activities consist of processing sensitive personal data on a large scale or a form of data processing which is particularly far reaching for the rights of the data subjects
 - Companies may name an employee as an internal DPO; or
 - appoint an external DPO.
- Public bodies must always appoint DPO

Data Protection Officer (DPOs) *(cont'd)*

- DPO duties include:
 - ☐ complying with all relevant data protection laws
 - ☐ monitoring specific processes, such as data protection impact assessments
 - ☐ increasing employee awareness for data protection and training them accordingly, and
 - ☐ collaborating with the supervisory authorities

Breach Notification

- Breach notifications are mandatory in all member states where data breach is likely to “result in a risk for the rights and freedoms of individuals”
- Businesses must notify authorities about any data security breach within 72 hours of discovering it - Article 33
- Businesses must also notify data subjects without *undue delay* after first becoming aware of a data breach - Article 34

Penalties

- Organizations that fail to comply with GDPR may be fined up to the *greater* amount of 4% of annual global revenue or €20 million (approx. \$23 Million)
- Tiered approach to fines –
 - Most serious infractions: For example, not having sufficient customer consent or violating core Privacy-by-Design concepts
 - ✓ up to 4% of annual global revenue or €20 million, whichever is greater
 - Lesser infractions: For example, not having records in order, not notifying authority and data subjects about breach, or not conducting privacy impact assessment (PIA)
 - up to 2% of annual global revenue or €10 million, whichever is greater
- Breach alone is not enough to merit a fine

Compliance

- All personal data processors and controllers of data subjects - regardless of their location - must comply with GDPR
 - ✓ *Broad interpretation* - companies may not have any direct relationship with Europe and still be subject to GDPR (indirect contact is sufficient). For example, a company based outside Europe that markets products to EU customers, tracks online behavior of EU users, or processes data on behalf of an EU client would still need to comply with the GDPR.

Compliance Practices

- All organizations holding and processing data subject personal data must comply with requirements by engaging in practices, such as –
 - ☐ Document all data processing activities that involve the collection, treatment, and safeguarding of personal data
 - ☐ Audit data they hold and develop a risk assessment
 - ☐ Ensure they have a DPO if necessary
- Build and improve processes and features to ensure all requests are quickly and effectively addressed when data subjects seek to exercise their rights
- If you are a data controller, review all sub-processors to confirm they have adequate security measures in place to protect personal data.
- Create a data breach reporting plan

Compliance Challenges

- GDPR imposes new responsibilities and duties
 - Companies must amend internal business organization process for compliance
- Intensive record keeping - controllers and processors are required to keep internal records of their data protection activities
- Major fines and sanctions for failure to comply
- Heavy cost – legal and compliance fees

Schrems II

- July 2020 decision from the Court of Justice of the European Union
- Invalidated the US-EU Privacy Shield
 - Closed off key mechanisms for transferring personal data from the EU to the US
 - *Schrems I* invalidated European Commission adequacy decisions with respect to EU-U.S. Safe Harbor
- CJEU was concerned with US government access to personal data for national security purposes and the rights of EU citizens in the US to judicial review and redress
 - CJEU found the U.S. was not according EU personal data the protection and rights of redress available in the EU
- International data flows can continue to be based on EU Standard Contractual Clauses if properly monitored

Standard Contractual Clauses

- Contract clauses promulgated by the European Commission to permit cross-border data transfers
- Essentially, companies outside the GDPR's reach voluntary agreements to comply with GDPR requirements to receive transfers including personal information from the EU
- The European Commission released new SCC's following the *Schrems II* decision
- Organizations must stop using the old SCC's in new contracts by September 27, 2021, and all existing contracts must be transitioned to the new SCC's by December 27, 2022

EU-US Data Privacy Framework

The European Commission adopted its adequacy decision for the EU-US Data Privacy Framework on July 10, 2023

- The Commission concluded that the US ensures an adequate level of protection (compared to the EU level) for personal data transferred to US companies participating in the Privacy Framework
- US Executive Order ensures data can only be accessed by US intelligence agencies only to the extent of what is necessary and proportionate
- EU individuals whose data is transferred will have the right to obtain access to their data, obtain correction or deletion of incorrect or unlawfully handled data, and are offered redress avenues in case data is wrongly handled
- US companies certify their participation by committing to comply with privacy principles such as purpose limitation as well as specific obligations concerning data security and sharing of data with third parties
- US Department of Commerce will process applications for certification and monitor compliance with participating companies – compliance is enforced by the FTC

Cross-Border Data Transfers Generally

Other data protection laws across the globe regulate the cross-border transfer of personal data

- Personal Information Protection Law (PIPL) of China
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- Personal Information Protection Act (APPI) of Japan
- The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules, or CBPR, is a government-supported privacy certification program that helps companies show they follow internationally recognized data protection standards.

GDPR: Seven Years In

- GDPR awareness

- Influx in data breaches and complaints
- Increase in data subjects exercising their information rights
- Organizations increasingly appointing DPOs
- Data protection legislation on the rise globally

- Enforcement

- Low enforcement to complaints/data breach ratio
- Not just about the fines – increase in warnings and reprimands
- Huge fines to huge companies: € 746 million (\$877 million) against Amazon in July 2021, €225 million (\$255 million) against WhatsApp, € 60 million (\$68 million) against Facebook in 2022, €50 million against Google (one of many fines against Google), €35 million against H&M in 2020

Data Breaches Increase

- 7.9 billion data records exposed in 2019 – a 33% increase from the same time in 2018 (source: <https://www.identityforce.com/blog/2020-data-breaches>)
- In 2020, 26 billion data records were exposed – the worst year on record (source: <https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020>)
- In August 2022, it was reported that the “Oktapus” hacker group had launched a months-long phishing campaign that compromised more than 130 companies, including Cloudflare, DoorDash, MailChimp, and Twilio
 - the attackers imitated the authentication service Okta to trick victims into entering login credentials on a fake authentication page
- In early 2025, LexisNexis Risk Solutions reported a data breach affecting about 364,000 individuals. The incident stemmed from a compromised third-party software platform used by the company, rather than its internal systems. LexisNexis discovered the breach in April 2025 and promptly launched an investigation, notified affected individuals, and implemented enhanced security measures.

Broad Definition of “Joint Controller”

- Two Facebook cases from the CJEU have led to a broad interpretation of when there are “joint controllers”
- “Joint Controller” situation arises when two or more controllers both have responsibility for meeting the terms of the GDPR
- Both controllers have full responsibility to ensure the entire process is compliant
- An individual can seek compensation from any joint controller (who may seek additional compensation from the other joint controller)

Vetting Service Providers

Practical Steps in Vetting:

- Use due diligence questionnaires for processor's IT and data security environment
- Ask for IT security certifications and policies
- Auditing
- Regular contract reviews and updates

Recent GDPR Enforcement Decisions

GDPR enforcement decisions in 2023:

- Meta GDPR fine of €1.2 billion in May 2023 – fine issued for the transfer of personal data from EU users to the US without adequate data protection mechanisms (Meta has appealed the fine)
- Amazon GDPR fine €746 million – fine issued after 10,000 people filed a complaint against Amazon in May 2018 through French privacy rights group – infringements in Amazon's advertising targeting system carried out without proper consent

EU Digital Operational Resilience Act (DORA)

- DORA is a new EU regulation that applies to financial services companies and is aimed at strengthening cybersecurity and digital resilience in the financial sector.
- It sets consistent rules for how financial institutions manage technology-related risks, report incidents, test their systems, and oversee third-party providers.
- DORA came into force on January 16, 2023, applied from January 17, 2025, giving companies a two-year period to prepare.
- This marks one of the most significant steps in the EU's ongoing effort to enhance digital resilience and complement the broader data protection framework established by the GDPR.

EU AI Regulation

- The EU Artificial Intelligence Act, or AI Act, is the first comprehensive legal framework for regulating artificial intelligence. It came into force on August 2, 2024, with requirements taking effect in phases through 2026.
- It classifies AI systems based on risk, banning the most harmful uses, such as some forms of facial recognition, and setting strict rules for high-risk systems.
- It also requires developers and providers, including those of generative AI tools, to be transparent about their data sources, training methods, and safety measures.
- The goal is to ensure AI is developed and used responsibly, safely, and in line with EU values.

GDPR: What Should Businesses do in Light of GDPR-Like Regulatory Trend?

- Continue to conduct general risk assessments
- Prioritize building programs with core fair information practices
 - E.g. Notice, consent, accountability, and transparency
- Keep up to date on regulatory developments specific to each country
- Consider participating in “sandboxes”
- Continue to foster culture of privacy by design and information security awareness in your business

Questions or Comments?

If you have any questions about this webinar that you did not get to ask during the live premiere, or if you are watching this webinar [On Demand](#), please do not hesitate to email us at info@financialpoise.com with any questions or comments you may have. Please include the name of the webinar in your email & we will do our best to provide a timely response.

IMPORTANT NOTE: The material in this presentation is for general educational purposes only. It has been prepared primarily for attorneys & accountants for use in the pursuit of their continuing legal education & continuing professional education.

*** This PowerPoint was produced in connection with a video webinar that premiered on [9/11/24](#). If you are reading this without the benefit of having attended, then you are missing its real value. You can access the webinar on-demand at [West Legal Ed Center](#) (for attorneys or accountants seeking CLE or CPE) or [Financial Poise](#) (for everyone else).

Meet The Faculty

Gabriel Buehler - gabriel.buehler@gmail.com



Gabriel is licensed in Washington and Idaho, serving the Pacific and Inland Northwest. My experience in business, product, marketing, and sales for the technology sector is what led me to the law. You won't find anyone else like me in the Pacific Northwest. [More info](#)

Julian Schneider - schneiderjulian@uclawsf.edu



Originally from Cologne, I began my legal career at a Berlin law firm specializing in press and media law. After earning an LL.M. in San Francisco and gaining experience in international data protection consulting, I now practice law in both Germany and the United States. In addition, I serve as an Adjunct Professor of Law at the University of California College of the Law, San Francisco (formerly UC Hastings), the oldest law school on the West Coast, where I teach courses on privacy law and AI compliance.

As a passionate soccer referee, to me, law is about fairness. Being dual-qualified in Germany and California, I regularly navigate complex cross-jurisdictional issues. My approach is to craft solutions that are tailored to each individual client and case. I am open to creative ideas, but I place equal value on reliable concepts. Active listening is central to my work. Substance beats style, and a well-defined problem is halfway to being solved. [Read More](#)

Alex Sharpe - alex@sharpellc.com



Alex Sharpe is a long-time Cybersecurity, Governance, and Digital Transformation expert with real-world operational experience. He has spent much of his career helping corporations and government agencies reap the rewards afforded by advances in technology while mitigating risk.

He began his career at the NSA before moving into the Management Consulting ranks building practices at Booz Allen and KPMG.

He subsequently co-founded two firms with successful exits, including The Hackett Group. Alex holds degrees in Business from Columbia Business School, Systems Engineering from Johns Hopkins University, and Electrical Engineering from New Jersey Institute of Technology (NJIT).

He is a published author, speaker, instructor, and advisor.

Thank you to our co-producer

THE NATIONAL LAW REVIEW

The National Law Review (NLR) is a premier legal news website offering in-depth analysis on a wide range of legal and business topics. Established in 1888, NLR has evolved into a **trusted resource** for legal professionals, business leaders, and the general public, providing timely and relevant information on legislative changes, court decisions, and regulatory developments

Visit *The National Law Review* to learn more
- <https://natlawreview.com/>

Comprehensive Coverage: NLR covers nearly every legal topic, including litigation, AI & the Law, employment law, IP Law, real estate, energy, health care, bankruptcy and much more.

Expert Analysis: Articles are authored by experienced attorneys and legal professionals, ensuring accurate and insightful commentary.

Daily Updates: NLR provides hourly legal news updates, keeping readers informed about the latest developments in the legal world.

About Financial Poise



The primary mission of Financial Poise™ is to provide reliable plain English business, financial, & legal education to individual investors, entrepreneurs, business owners, & executives, & to help trusted advisors do the same.

*Newsletter subscribers are occasionally offered free webinars. Subscribers never receive more than one email per week & their information is never shared.

Sign up for our free weekly e-newsletter [here](#)*.

Learn how to write or speak for Financial Poise [here](#).
The antithesis of “pay-to-play.”

Check out our other webinars [here](#).

Send any other inquiry to info@financialpoise.com