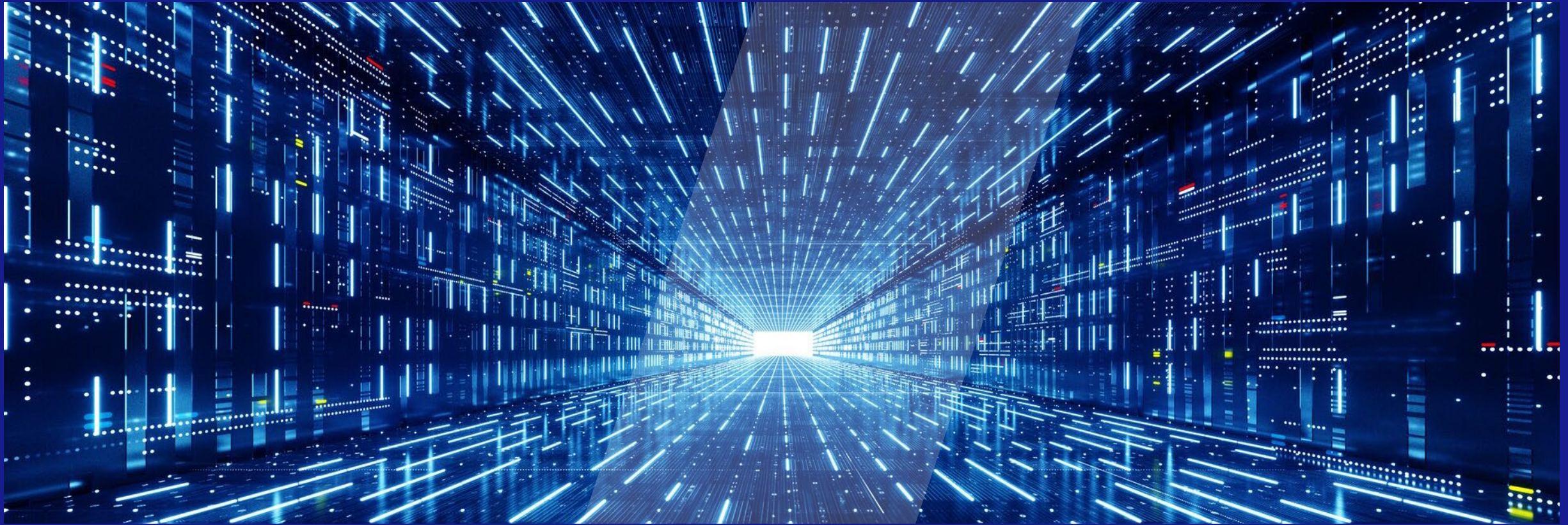




Why Should US Orgs Certify Their GDPR Compliance?

A practical path to GDPR assurance & EU data transfer confidence

September 2026

forv/s
mazars

Agenda

1. Introductions
2. Context & Challenge
3. What Is Europrivacy & Why Does It Matter?
4. Key Business Benefits
5. How Certification Works
6. Discussion & Next Steps



01

Introductions



Today's Presenters



Alan Gutierrez-Arana

Principal • Forvis Mazars, LLP



Liam McKenna

Partner • Forvis Mazars in Ireland



Sébastien Ziegler

CEO • Europrivacy



Giovanni Francescutti

Global Technical Manager • DNV

02

Context



Context

Obligations of US & EU Organizations Processing Data Under GDPR

The GDPR applies to EU organizations that process personal data.

European organizations remain accountable for GDPR compliance, even when personal data is processed by a third-party provider. Where a US service provider processes EU personal data without appropriate GDPR safeguards, the European organization may face regulatory enforcement, fines, litigation, remediation costs, and reputational damage. Responsibility cannot be outsourced.

The GDPR also applies to US organizations offering goods and services in the EU or monitoring behavior in the EU.

US organizations subject to the GDPR may be required to designate an EU representative if they do not have an applicable office or establishment in the EU.

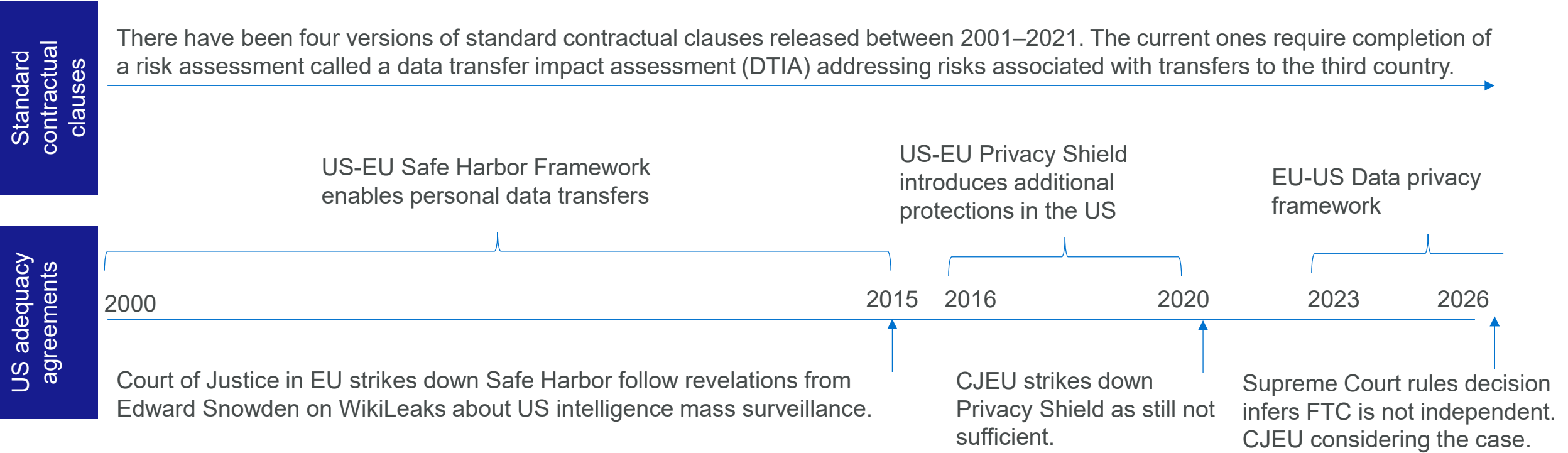
In practice, US organizations that are processing personal data of EU data subjects will either have a direct or indirect obligation to comply with the GDPR.

Regulatory fines up to \$23,000,000 or 4% of global turnover may be imposed and data subjects can take civil actions where their data is not managed in compliance. Since 2018 fines of between \$7–8 billion have been applied.

Context

Challenges for US & EU Organizations Presented by Data Protection Law

Europe implemented its first data protection directive in 1995. Within the directive there was a requirement on data controllers to only transfer personal data to a third country (such as the US) where adequate protections are provided. European organizations may avoid doing business with US firms rather than deal with the perceived compliance risk.



Europrivacy can help address challenges and unblock commercial relationships with EU prospects.

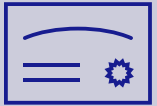
03

What Is Europrivacy & Why Does It Matter?



What Is Europrivacy?

Europrivacy is the first European Data Protection Seal approved by the European Data Protection Board (EDPB).



First pan-European Data Protection Certification approved by EDPB and only one available internationally



Recognized across all 30 EU and EEA member states with legal effects and benefits



Certifies specific processing activities, including in products and services

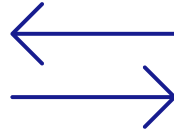


Supports GDPR compliance & accountability

Why Europrivacy Matters to US Organizations



Facilitates EU data transfers
and market access



Reduces risks and due diligence
costs, with higher protection
compared to SCCs



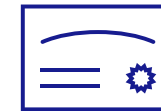
Recognized by regulators in
enforcement decisions



Independent accredited audit



Article 46 transfer mechanism



Annual surveillance, 3-year cycle

EDPB Opinions & Impact for U.S. Organizations

April 2026 Decisions

On April 15, 2026, the EDPB adopted two pivotal opinions that significantly evolve the scheme.



April 2026:

- **EDPB extends Europrivacy certification internationally.**
US companies now can obtain the same European Data Protection Seal previously available only to EU/EEA entities.
- **EDPB approves Europrivacy as a mechanism for international data transfer under Art. 46 GDPR.**



- **Legal weight:** Certification is referenced **73 times** in the GDPR, carrying formal recognition with legal effects and benefits.
- **New international data transfers tool based on effective compliance assessment,** less risky than SCCs.
- **Expected to become a growing factor in future procurement policies.**



- **Reduction of risks for all parties.**
- **Simplifies compliance management.**
- **Turns regulatory compliance into a competitive advantage,** and potential source of value creation and revenues.
- **Can be used in procurement policies to reduce risks, costs, and efforts:** by requesting your service providers to be GDPR-certified.

04

Benefits of Europrivacy



Key Business Benefits

Competitive Differentiator

Europrivacy certification signals a verified commitment to protecting EU personal data, strengthening customer trust and openness. Customers that are concerned about their data may prefer certified organizations.

Reduced Risk

Demonstrable GDPR assurance reduces exposure to regulatory penalties and the legal and financial fallout of data mishandling. The GDPR specifically requires supervisors to recognize efforts to meet compliance obligations through certification.

Compliance

Independent third-party certification gives internal stakeholders clear, auditable evidence that EU data obligations are being met.

Unblock Sales

Accelerate EU customer acquisition by reducing privacy-related procurement barriers. Europrivacy certification provides independent assurance that helps EU controllers assess and engage US processors more quickly, with lower perceived risk and reduced due diligence effort.



05

How Certification Works



How Certification Works



Define Target of Evaluation (TOE)



Conduct gap analysis & remediation



Prepare documentation & evidence



Independent audit by certifying body



Communicated with the Data Protection Authorities (for GDPR endorsed schemes)



Certification issued & maintained

Typical Certification Journey

Preparation

Define the TOE and run a gap analysis that benchmarks current practices against Europrivacy requirements.

Gap Analysis

Identified gaps are remediated and the supporting documentation and evidence are prepared for assessment.

Applying for Certification

ToE validation and review.

Third-Party Independent Audit

An accredited certifying body conducts an independent audit, after which Europrivacy certification may be issued.

Maintaining Certification

Certification is maintained over time through ongoing monitoring and periodic surveillance audits.



How Deep Is the Audit?

On top of the document analysis ...

Document Reviews

Consist in analyzing the relevant documentation related to the ToE.

Interviews

Consist in meeting relevant stakeholders to ask questions and request clarifications. The interviews have been performed through.

Data/Records Sample Analysis

Refers to the process of examining a subset of data or records to draw conclusions about the entire dataset.

Examinations

Refers to the visit or remote assessment of premises where data processing is performed or managed, and to the direct observation of objects or systems relevant for the ToE.

Testing

Tests refer to the performance of a data processing or procedure in order to verify and determine if requirements specified in the criteria are effectively met (e.g., testing a process as a user).

06

Discussion



Discussion & Next Steps

Where are your biggest challenges today?

Which processes could be certified first?

How can certification support your EU growth strategy?

Contact us to explore a readiness assessment.

How Forvis Mazars Can Help

Europrivacy GDPR certification can help support cross-border data transfers, streamline conversations with EU clients, and provide independently verified evidence of compliance.

Forvis Mazars:

- Global consulting partner for Europrivacy
- Gap assessment & readiness support
- Remediation and documentation assistance
- End-to-end certification support

Scan to learn more.





Europrivacy
Services

Is Your Org Ready?

Contact

Forvis Mazars

Alan Gutierrez-Arana
Principal • Forvis Mazars, LLP
P: +1 267 342 1286
alan.gutierrezarana@us.forvismazars.com

Liam McKenna
Partner • Forvis Mazars in Ireland
P: +353 86 380 5472
liam.mckenna@forvismazars.com

Scan to learn more.



The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.

