

Data Protection and Privacy 2022

Navigating Opportunities and Challenges:
Cross-border Data, the Cookiepocalypse and
Standard Contractual Clauses





David Naylor

London

david.naylor@squirepb.com



Dr. Annette Demmel

Berlin

annette.demmel@squirepb.com



Malcolm Dowden

London

malcolm.dowden@squirepb.com



Bartolome Martin

Madrid

bartolome.martin@squirepb.com



Kyle Fath

Los Angeles

kyle.fath@squirepb.com



Francesco Liberatore

London, Brussels and Milan

francesco.liberatore@squirepb.com

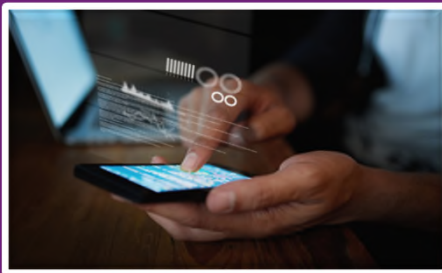
GDPR: European Law, Global Reach?



How does GDPR affect your organization, and how can EU data protection authorities affect your business?



What steps can we take to safeguard the flow of business-critical data across borders?



What does the future hold for data protection, privacy and cybersecurity?

Is Your Organisation Processing Personal Data?

- GDPR includes an extremely broad definition of “personal data”
 - any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- And of “processing”
 - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



- GDPR has been incorporated into the laws of the UK and there are mutual “adequacy decisions” allowing transfers of personal data between the UK and the EU/EEA.
- Brexit does mean that there are some different or additional UK GDPR compliance obligations when personal data is processed in a way that involves both EU/EEA and UK including additional documentation.
- Queen’s Speech May 2010 set out the UK government’s legislative agenda and includes a Data Bill to reform, including proposals relating to Data Privacy Impact Assessments (DPIAs), cookie banners and the requirement to appoint Data Protection Officers (DPOs).



Trans-Atlantic Data Privacy Framework: The Solution to Schrems II?

- *Schrems II* European Court ruling July 2020 found EU adequacy decision in relation to the EU-US Privacy Shield unlawful.
- The EU and US have reached agreement in principle on a revamped Privacy Shield data transfer agreement.
- Political agreement will have to be translated into legal text, agreed by EU data protection authorities and adopted by the EU Commission.
- Some EU data protection authorities (eg Austria) have been taking a hard line on “risk-based” transfer impact assessments, focusing on concerns relating to US Federal surveillance powers (FISA 702, EO 12333).
- Will “in principle” political agreement become effective legal protection?
- What steps can we take in the meantime to ensure lawful transfers of personal data?



- Although headlines tend to focus on GDPR fines, they are not the only sanctions available to supervisory authorities, and in terms of business impact they might not be the most significant.
- Data protection authorities (including Portugal and France) have indicated a willingness to issue “stop” orders, including orders blocking the use of tools such as Google Analytics.
- Data Protection authorities (Netherlands) have issued initial fines coupled with ongoing weekly fines to incentivize rapid improvement in policies, procedures and practices.
- Data Protection authorities (Poland) have issued fines where contractual protection (e.g., audit rights in respect of processor security measures) have not been exercised. Contractual protection alone will not be enough.
- UK data protection authority has imposed (sometimes significant fines) for infringements including data breaches, unlawful sharing of data and unsolicited direct marketing.
- What can we learn from these recent trends in enforcement action?



- In January 2022 the EDPB published its [Examples regarding Personal Data Breach Notification](#), addressing commonly-encountered scenarios including ransomware and data exfiltration attacks.
- Key messages include:
 - Data breaches not limited to hacking and ransomware attacks;
 - Backup, failover and risk mitigation are crucial elements of your data compliance strategy;
- What steps can we recommend to reduce the risk of having to report personal data breach?



2022: Surviving the “Cookiepocalypse”

- Google’s announcement (March 3, 2021):
 - "Today, we're making explicit that once third-party cookies are phased out, we will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products," (David Temkin, Google's director of product management, ads privacy, and trust).
- What is the “cookiepocalypse”?
- What does the phasing out of third-party cookies mean in practice?



E-Privacy Regulation

- Strengthen privacy rules for providers of electronic communications services
- Not expected to enter into force before 2023 and come into effect before 2025
- If adopted:
 - Simpler rules on cookies
 - protection against spam
 - more effective enforcement
- In the meantime, interaction of EECC and ePD means extension of ePD to NI-ICS

Why?

- **Market contestability.** The network effects of data aggregation make digital markets subject to tipping in which a winner will take most of the market, and this risks choking competition and innovation.
- **Effectiveness.** Antitrust law may not be sufficient to deal with data aggregation.
- **Internal market objectives.** New regulations will be directly applicable across the EEA, to avoid a patchwork of regulations and promotes a single market across the EEA.

Other future developments: new digital markets regulations – a complex framework!

Proposed regulations, expected to come into force between 2023 and 2024

- Data Act
- Data Governance Act
- Artificial Intelligence Act
- Digital Markets Act
- Digital Services Act
- European Data Spaces
- Standards Initiative



Legislation already in force

- Database Directive
- GDPR
- Free Flow of Non-Personal Data Regulation
- Platform to Business Regulation
- Open Data Directive
- Electronic Communications Code

Data mobility, switching, interoperability, FRAND terms

Compliance strategy must take account of the interplay between these regulations and EU/national competition laws – examples: Data sharing must still comply with competition law safeguards; and the same conduct may be subject to parallel enforcement

For those of you who require CLE credits please note the following states have been approved for 1.0 hour of CLE in **AZ, CA , NJ, NY, OH and TX.**

Please write down the following affirmation code **[Cookie523]**

Within a couple of business days, you will receive an email with a ***uniform certificate of attendance*** and ***program evaluation*** to complete and SUBMIT to my colleague, Robin Hallagan at robin.hallagan@squirepb.com.

The firm with local connections and global influence

Benefits for our clients

- Access to new knowledge, new markets and new expertise
- Greater global influence and reach, combined with powerful local insight
- Better problem-solvers because of the additional knowledge and expertise
- Deeper relationships with clients
- Stronger connectivity between government, law and business
- Stronger global government relations
- A deeper bench of lawyers in more key places

Global Coverage

Abu Dhabi	Manchester
Atlanta	Miami
Beijing	Milan
Berlin	Moscow
Birmingham	New Jersey
Böblingen	New York
Bratislava	Palo Alto
Brussels	Paris
Cincinnati	Perth
Cleveland	Phoenix
Columbus	Prague
Dallas	Riyadh
Darwin	San Francisco
Denver	Santo Domingo
Dubai	Seoul
Frankfurt	Shanghai
Hong Kong	Singapore
Houston	Sydney
Leeds	Tampa
London	Tokyo
Los Angeles	Warsaw
Madrid	Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico

■ Office locations
■ Regional desks and strategic alliances

