Morgan Lewis

GDPR HOT ISSUES:
COOKIES, DATA TRANSFERS, AND ENFORCEMENT TRENDS

September 17, 2020

Presenters

Pulina Whitaker

Dr. Axel Spies

Andrew J. Gray IV

Morgan Lewis

Our Discussion

- GDPR continues to be a hot topic and a ripe area for enforcement
- Data transfer – how to do it
- Brexit remains an unknown from a privacy perspective – will the UK obtain an adequacy decision
- ePrivacy laws regarding cookie consent requirements is a growing area of enforcement activity
- Schrems II – consequences for data transfers
- ePrivacy Regulation still not published
- German approach
- European privacy enforcement activity
- Collective actions for privacy breaches

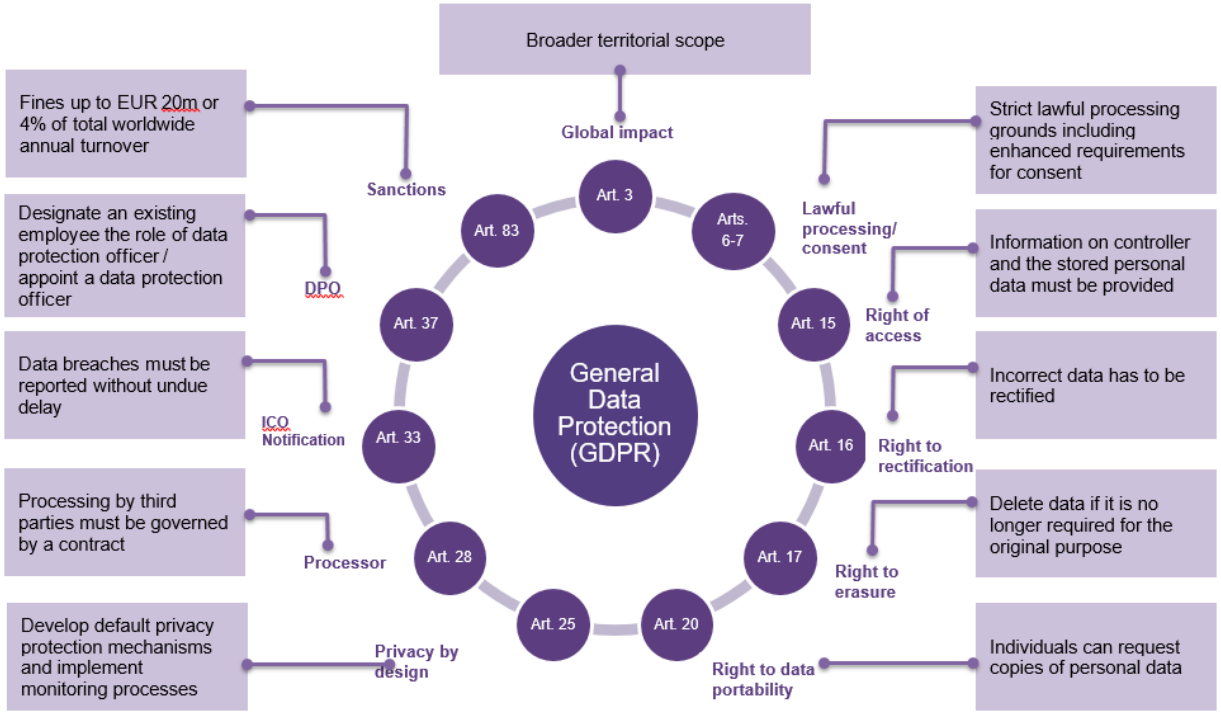
The EU General Data Protection Regulation

- EU GDPR came into effect on 25 May 2018
- Local EU and UK data protection laws supplement the GDPR
- The GDPR applies to controllers and processors having an EU-based establishment where personal data are processed in the context of the activities of this establishment
- The GDPR also applies to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:
    - the offering of goods or services (regardless of payment)
    - the monitoring of data subjects' behavior within the EU
- "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
- Personal data has to be processed fairly and lawfully – transparency is key e.g. privacy notices

The EU General Data Protection Regulation, cont'd

- Data Protection Officer: for controllers/processors processing substantial sensitive personal data or who have core activity of monitoring individuals on a large scale or public body
- Right to request to be forgotten, have data rectified or deleted
- Privacy by design: privacy safeguarding technology built-in from the start
- Actively factor privacy considerations into the design and upgrade of all systems, policies, settings which process personal data
- Privacy by default: privacy-friendly default settings until user chooses otherwise
- Data protection impact assessment: prior to processing if high risk for individuals
- Controllers must notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be high risk to individuals
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000
- Controllers and processors are both directly liable under GDPR

Overview of the GDPR



Data Transfers under GDPR

- General restriction on transferring personal data outside EEA to a "third country"
- Adequate countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay
- GDPR permitted data transfer options (safeguards):
  - Binding Corporate Rules
  - Standard contractual clauses: importer controller/processors based in the third country; exporter controller must be based in Europe
  - Importer subject to an approved Code of Conduct
  - Importer subject to an approved certification mechanism
  - No longer the Privacy Shield after Schrems II
- GDPR permitted derogations:
  - Explicit consent
  - transfer is "necessary" for performance of contract; to establish, exercise or defend legal claims; from a public register
  - Where the transfer is not repetitive, concerns a limited number of data subjects, is necessary for compelling legitimate interests of controller (not overridden by data subject rights) and safeguards in place to protect the data

Data Transfers - SCCs

- Standard contractual clauses (to processors or controllers) are a very common method of transferring data outside the EU
- The European Commission has consistently emphasised the need for data transfers to be possible for economic purposes
- In Schrems II, the processor SCCs were validated
- The ECJ made clear that the laws of the importer were relevant to assess if the importer can meet its obligations under the SCCs
- If there is a risk that the importer has legal obligations that could undermine the SCCs obligations, the transfer may need to be suspended unless additional safeguards can mitigate against these risks – we await EDPB guidance on additional safeguards
- Encryption; restrict access; consider if transfers are necessary; localise?
- Transfers to the US will not, necessarily, invalidate the SCCs for importers in the US – a risk assessment may be needed
- If the importer cannot comply, the transfer must be suspended or terminated – notify the supervisory authority

Which data transfer option?

- Privacy Shield – no longer valid for EU to US transfers – DoC says to continue to abide by commitments as do some European supervisory authorities; no grace period so invalid from July 2020; no point renewing!
- Standard contractual clauses – easy to execute; not so easy to implement
  - Need to consider legal framework in importer's country;
  - Consider additional safeguards e.g. encryption in transit and at rest;
  - Importer to notify exporter if it cannot comply with SCC obligations
  - Exporter or supervisory authority can suspend data flow pending EDPB approval of the transfers continuing
- BCRs – time and expense to get approval
  - EU supervisory authorities take several years to approve
  - UK approved BCRs need to be approved by an EU supervisory authority before end of Brexit transitional period (31 December 2020)
- Consent – GDPR standard of explicit consent
- Other new options: Code of Conduct, privacy seals – details awaited from supervisory authorities
- Give notice to data subjects of the transfers

UK Data Protection Act 2018

- UK Data Protection Act 2018 – in force on 25 May 2018
- Implements local law permitted provisions of GDPR:
  - children's consent at 13 years;
  - processing for criminal records;
  - exemptions from restrictions for processing special categories of interest e.g. public interest exemptions;
  - exemptions from subject access rights
- Includes law enforcement processing and intelligence services processing provisions
- Sets out powers of enforcement of ICO

BREXIT AND UK DATA PRIVACY

- UK has left the EU – transitional period until 31 December 2020
- UK GDPR will be implemented to give direct effect to GDPR
- Until we receive an adequacy decision, the UK will be a third country (like the US) – data exports from the EEA will be restricted – SCCs etc will be needed
- Other data privacy laws already incorporated in UK law e.g. ePrivacy Regulations give effect to Electronic Communications Directive
- ICO has approved current EU SCCs for data transfers from the UK – likely to be replaced in future with UK versions; EU will also release replacements to the current SCCs for GDPR purposes (long awaited)

COOKIES

- Cookies collect a vast array of personal data (including some IP addresses will be personal data under the GDPR)
- Opt-in consent needed for non-essential cookies e.g. analytics
- Planet49 case – active consent
- GDPR standard of consent: freely given, fully informed, express/active
- Tracking technologies are a point of concern for EU authorities
- EU Privacy Regulation still not in force…

Key Takeaways

- Schrems II – consider risks and measures to mitigate against the risk: is there an alternative to the proposed transfer if you need to suspend
- Brexit – the UK will be a "third country" with restrictions on data exports from the EEA unless we receive an adequacy decision by the end of 2020
- Cookies – obtain active consent to non-essential cookies for European users (unless the site is not intended for a European audience)

Morgan Lewis

LIFE AFTER THE EU PRIVACY SHIELD AND OTHER CONSEQUENCES OF THE LANDMARK CJEU "SCHREMS II" DECISION

A few basics on EU-US data transfers

- The transfer of data from countries within the European Economic Area (EEA) to third countries → restrictions within the EU General Data Protection Regulation ("GDPR").

Background

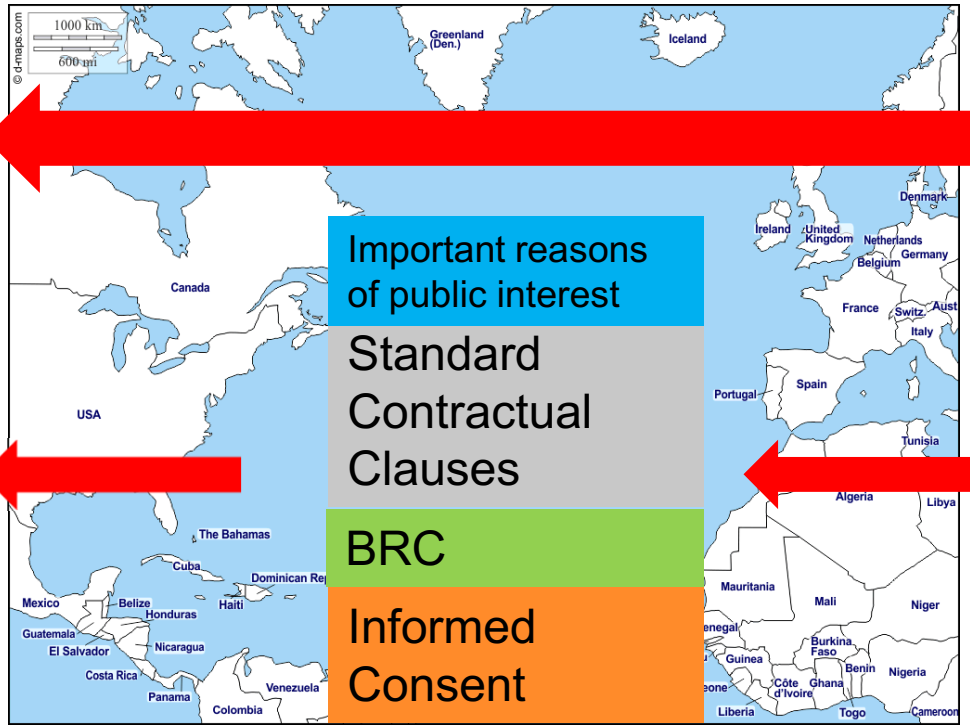
- The GDPR broadly prohibits the transfer of personal data to so-called "third countries", subject to certain exceptions.
- One such exception where the European Commission has made an 'adequacy decision': a finding that the receiving country has in place adequate protection for the rights and freedoms relating to individuals' personal data, equivalent to those available within the EU.
- US was deemed **not** to provide protections equivalent to those available in the EU.
- US Department of Commerce and the European Commission devised the **Privacy Shield** in 2016/17 as a set of principles designed to ensure equivalent protection via self-certification.

The Data Transfer World from the EU before July 16, 2020

Privacy Shield
- EU/US
- Swiss/US

Data Importer

Pro-cessor



Important reasons of public interest

Standard Contractual Clauses

BRC

Informed Consent

Pro-cessor

Data Exporter

Morgan Lewis

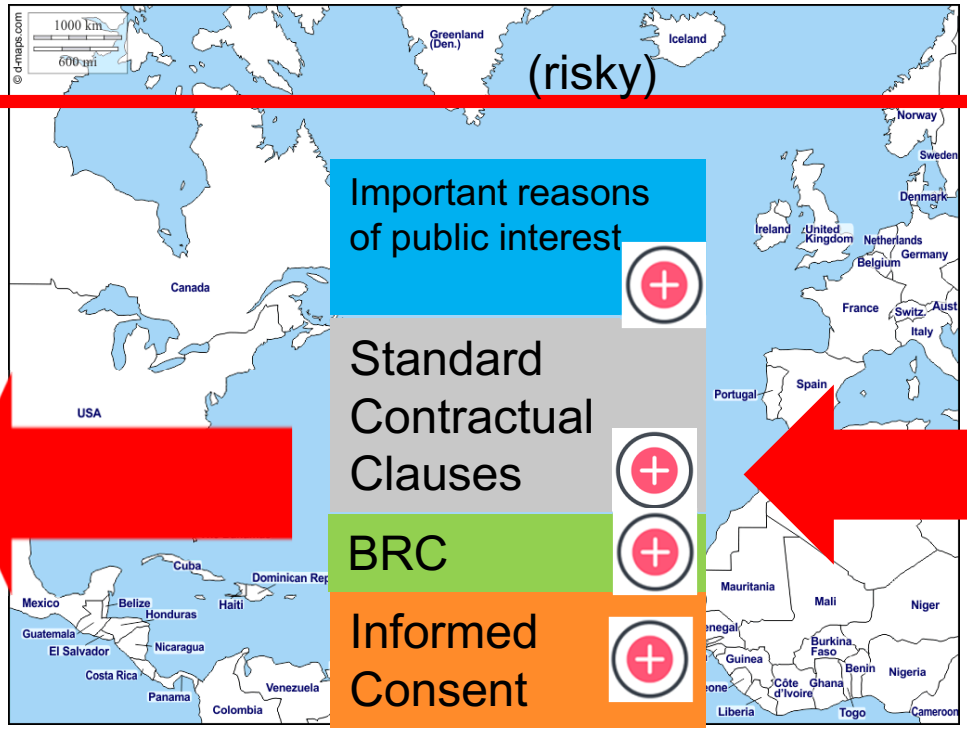
Enter Mr Schrems → CJEU "Schrems 2"

The Data Transfer World from the EU After July 16, 2020

Privacy Shield
~~EU/US~~
- Swiss/US

Data Importer

Pro-cessor



Pro-cessor

Data Exporter

Morgan Lewis

CJEU Case C-311/18 - "Schrems II"

16 July 2020→ Court of Justice of the European Union (CJEU) → judgment (ruling):

- EU Privacy Shield Framework decision for data transfer between the EU **is invalid from the EU perspective**
- **No grace period**
- Reducing the available options for the sharing of personal data between the two regions.
- "**Additional measures**" may be required before companies may rely on traditional means to justify international data transfers.

Data Exporters and Importers:

- risk balancing exercise with insufficient guidance from the DPA → **they want a case-by-case analysis and not only for EU-US data flows.**
- fine line between compliance with their obligations under GDPR and their need to export data outside the EEA to conduct their business.
- **Sep. 9**: **Irish DPA** plans suspension of FB's EU data flows to the U.S. (WSJ and others.). Time line unclear.

CJEU Schrems 2

- Immediate effect for all US companies receiving data.
- **US Secretary of Commerce Wilbur Ross**: U.S. will continue to administer the program. Decision "does not relieve participating organizations of their Privacy Shield obligations."
- The U.S. Department of Commerce and the European Commission have **initiated discussions** to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with Schrems 2.

Joint statement: "The European Union and the United States recognize the vital importance of data protection and the significance of cross-border data transfers to our citizens and economies. We share a commitment to privacy and the rule of law, and to further deepening our economic relationship, and have collaborated on these matters for several decades."

- Could lead to "Schrems 3." → **data exporters caught in the middle.**

CJEU Schrems 2 – Can I rely on "Derogations"?

Derogations under Art. 49 (1) GDPR

- (a) Explicit consent?
- (b) "Necessary data transfer for the "performance of a contract.

Article 49 GDPR remains available in certain situations (*Schrems II*, para 202), but the European data protection authorities have already indicated that they will continue to take a narrow view

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, as published on 25 May 2018. → "**Occasional**" data transfers only.

- Some large US companies still seem to rely on these derogations.
- Not clear what "occasional" means; only mentioned in GDPR Recitals.

CJEU Schrems 2 – Are SCCs a way out?

CJEU warns against a sign and shelf use of Standard Contractual Clauses

- As EU-US Privacy Shield is off the table….
- companies must ensure a legal basis for all international data transfers
- Most commonly, companies seek to rely on Standard Contractual Clauses ("SCCs").
- SCCs permit international transfers of personal data where the sender and recipient have entered into a contract adopting model clauses drafted by the European Commission that provide individuals with directly enforceable rights against the parties to the contract.

CJEU Schrems 2 and SCCs

- CJEU The SCCs generally remain a valid mechanism for data transfer (*Schrems II*, para 149)
- BUT… there are circumstances in which the SCCs might not constitute a sufficient means of protecting the right to data privacy, in particular where the law of the recipient country "allows its public authorities to interfere with the rights of the data subjects to which that data relates" (*Schrems II*, para 126).

→ **The CJEU's concerns are mostly about US surveillance and how individuals in the EU can defend themselves against it.**

Ironic side note: Europeans cannot invoke the GDPR or the Charter of Fundamental Rights when dealing with European intelligence services.

→ **Revised SCCs – when? End of the year?**

E. Snowden

CJEU Schrems 2 - SCCs

Consequences for the use of SCCs:

- Burden is on the data exporters who may need further information from the data importers.→ Additional safeguards on top of the SCCs (Schrems II, para 132)?
- Data transfers to the US under SCCs are not necessarily invalid because of Schrems II, but the **ability of the importer to comply with the SCCs has to be assessed**;
- Where there is **a substantive concern** that the importer (in any location, not just the US) is unable to comply with the SCCs, additional safeguards need to be considered;
- The SCCs require that data transfers to an importer have to be suspended or terminated if the importer cannot comply with the SCCs and the supervisory authority must be notified.

To Summarize: Practical Effects of Schrems 2

- The *Schrems II* decision is **binding on all authorities and courts** of the EU member states, which have to deal with this question in accordance with the CJEU decision.
- **Transfers using Privacy Shield** as the transfer mechanism **are illegal from the EU point** and could trigger fines and claims for damages.
- **Transfers based on Standard Contractual Clauses are conceivable, but** may not the requirements for an effective level of protection as required by the CJEU. → Risk assessment.
- **Using Article 49 derogation may be possible, but** is subject to the innate limitations of such mechanism (e.g. necessity, occasional transfers only etc).

And what about the Swiss-US Privacy Shield?

- Switzerland is no bound by any CJEU judgement.
- **Sept 8**: The Swiss DPA (FDPIC) released its own statement on the Swiss US Privacy Shield and SCCs.
- Very similar to the Schrems 2 CJEU decision and the European Data Protection Board's Guidelines.
- Difference: FDPIC has no authority to annul the Privacy Shield decision of the Swiss Government.
- "*At present, there is no comparable court decision [as Schrems 2] in Switzerland. It is therefore open whether Swiss courts will apply Art. 6 of the Swiss Privacy Act with regard to data access by US authorities to be similar to the conclusions would be reached in application of the GDPR as the CJEU.*"

→ **Relying on the Swiss-US Privacy Shield alone is probably risky.**

Some Practical Steps for data exporters

- **What To Do…**

➢ Take inventory of all your data transfers.

➢ **Contact your service provider** in the third country and inform them of the CJEU decision.

➢ **Obtain information on the legal situation** in the third country (including as with respect to surveillance).

➢ Check whether there is an **adequacy decision** for the third country.

➢ Check whether you use the **Standard Contractual Clauses** for your transfer.

➢ Check whether there are any **supplementary measures** that can be adopted

→ **"SCC Plus" suggested.**

SCC Plus Recent Suggestions by the German DPA

- 8/ 24: A German Data Protection Supervisory Authority (Baden Wurttemberg – LfDI) now requests specific amendments to "Controller-to-Processor" SCC when transferring data to "unsafe" third countries such as the U.S.
- Similar amendments to the "Controller-to-Controller" SCC ?
- The LfDI also wants that the controller (data importer) offers additional guarantees that effectively prevent access by the US secret services and thus protect the rights of the data subjects, such as
- "*Encryption where only the data exporter has the key and which cannot be broken even by US [secret] services*" → ***?!?***
- *Anonymization or pseudonymization, where only the data exporter can perform the assignment…*" → ***?!?***

SCC Plus (2)

- The LfDI wants the parties to agree to the following SCC amendments:
- **Amendment Annex Clause 4f**: Informing the data subject, not only when special categories of data are transferred, but also in the case of any transfer (before or as soon as possible after the transfer) that hi/ hers data will be transferred to a third country which does not provide an adequate level of protection within the meaning of Regulation (EU) 2016/679 = GDPR.
- **Amendment Annex, Clause 5d i**: obligation of the data importer to inform not only the data exporter but also **the [individual] data subject** without delay of any legally binding requests by an enforcement authority to disclose the personal data; if this disclosure is prohibited by other means, for example by a criminal law prohibition to maintain the confidentiality of criminal investigations, the data exporter must contact the LfDI supervisory authority to clarify the further procedure.
  - **Critic by Commenters: In most controller-processor relationships, the processor is unable to comply with this requirement because they have no direct relationship with the individuals.**

SCC Plus (3)

- **Amendment to Annex Clause 5d** of an obligation on the data importer to take legal action against any disclosure of personal data and to refrain from disclosing personal data to the relevant authorities until a competent court of last instance has ordered the data importer to disclose the personal data
- **Amendment to Annex, clause 7(1), addition to (b)**: referral of the dispute to the courts of the Member State where the data exporter is established in the event that a data subject claims rights as a third party beneficiary and/or damages against the data importer under the contractual clauses.

SCC Plus (4)

- Inclusion of a compensation clause:

"Liability

The parties agree that if one party is held liable for a breach of the clauses committed by the other party, the second party will compensate the first party for all costs, damages, expenses and losses incurred by the first party to the extent that the second party is liable. The compensation shall be subject to (a) the data exporter notifying the data importer immediately of any claim for compensation and (b) the data importer being given the opportunity to cooperate with the data exporter in defending the claim for compensation or agreeing on the amount of compensation."

Agreement that the data be solely hosted in an EEA member state?

- Probably a good idea to mitigate the risk
- **But** there is usually some data access from the U.S.
- US representatives or affiliates with "*possession, custody or control*" (Federal Rule of Civil Procedure 34(a))
- An agreement that no data be transferred to the U.S. altogether?
- While service providers may still have remote access to personal data located on servers in the EEA, the risks associated with mere remote access are probably lower than storing the data on servers located in a country outside the EEA.

EDPB Draft Guidelines on data controllers and processors (issued Sept 2)

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

- Practically important because there are no SCCs for processors in the EU and controllers in the third country.
- Joint controllers:

> *[…] as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so."*
> ***BUT:*** *"the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing…"*

- **Example:** clinical trial: Sponsor, CRO, investigator.

Will there be a political solution?

- German industry Groups (ZGV) have written Angela Merkel (08/22).
- EU presidency

US Sec. Wilbur Ross on Schrems 2: "*The Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. Today's decision does not relieve participating organizations of their Privacy Shield obligations*."

- Pressure may mount with recent action of Irish DPA

What's next for privacy compliance?

Welcome to the EU ePrivacy Regulation and cookie consent

Morgan Lewis

EU ePrivacy Regulation

Why is it necessary at all? Don't we have enough to do with the GDPR?

- EC argues that the "old" ePrivacy Directive 2002/58/EC must be overhauled to bring it into compliance with the GDPR for the "electronic communications" sector
- **Extraterritorial**: Scope → data processed in connection to the provision of electronic communications services provided to end users located in the EU, even if the provider is established outside the EU (Art. 3)
- The ePrivacy Regulation will be **directly applicable** in the EU member states
- **Implementation period**: probably one year.

What does it cover?

- In particular, cookie use, user tracking, processing of meta data (legitimate interest).

EU ePrivacy Regulation (2)

Why is it still pending more than two years after the GDFP entered into force?

- There was no agreement in the EU Council of Ministers, negotiations stalled end of 2019
- Croatia (EU Presidency) presented a new draft but ran into further roadblocks.
- Germany (EU Presidency as of July) took over
- Main bone of contention: what to do with cookies (cf. EU Cookie Directive 2009/136 EC)?
- Planet 49 Decision of CJEU of 1 October 2019 on the use of cookies.

EU ePrivacy Regulation (3)

- Does it apply to Machine-to-Machine or Internet of Things services?

DRAFT Recital 12:
"The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. […] it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications."

- **Opposition:** The data exchanged between the machines themselves, does not aim to capture information about the private life of the operator using the machine/ device but exclusively about the machine itself.

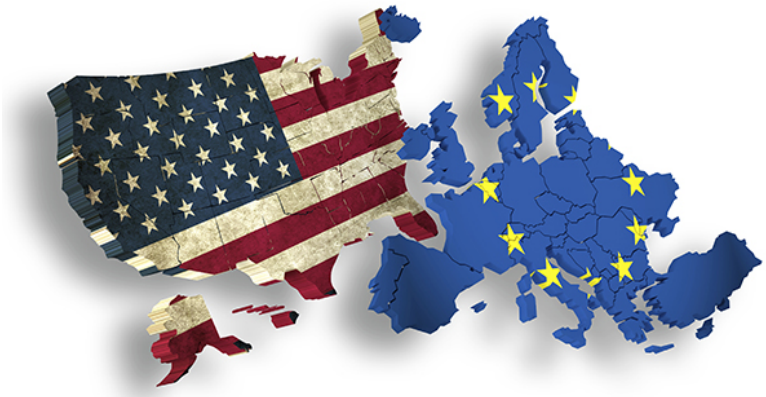
National legislatures advance the cookie issue: Example: Germany - Section 9 TTDSG-E

- Section 9 (1) → access to the end user's terminal equipment in order to store information there or to read out stored information may only take place with the end user's consent.
- Section 9 (2) → exceptions. Consent is not required if
  - the storage of information on the terminal equipment or access to information already stored is **technically necessary** to transmit communication via an electronic communications network or
  - to provide Telemedia that the **end user has requested**.
- Section 9 (3) → rules on what constitutes an **active consent.**
- Section 9 (4) clarifies that consent can also be given through browser settings or other online procedures for consent management (e.g. through data trustees). ← **Compatible with the EU ePrivacy Directive?**

→ **Other EU Member States may have different approaches.**

Key Takeaways for US Data Importers

- Check your international data transfer agreements
- Be cooperative (risk assessment)
- Follow the developments re Schrems 2
- Be prepared for new laws (ePrivacy Regulation, national laws)
- Document, document, document.



European Enforcement Activity

- A number of cases are coming through the courts for privacy breaches – mostly against Big Tech
  - Lack of transparency i.e. inadequate notices
  - Data security issues – e.g. BA
  - Implied, not express, consent from users to data collection and secondary use of the data
  - Cookies: real-time bidding, double click ad cookies
  - Browsers collect excessive data and share data with third-parties for marketing purposes
- Cases are being brought on a collective/representative basis – under existing laws e.g. UK group litigation orders
- New EU Representative Actions Directive – due to come into force in next year or two

Biography

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment. She is a co-Head of our global Privacy & Cybersecurity practice. She manages employment and data privacy issues in sales and acquisitions, commercial outsourcings and restructurings. Pulina provides day-to-day advisory support for multinationals on the full spectrum of data privacy issues, including data breaches, data protection compliance issues and data sharing and data transfer arrangements. Pulina has deep experience managing international employee misconduct investigations as well as cross-border data breach investigations. She has been appointed as a Compliance Monitor for the UN and for USAID. She is also a Trustee of Hostage International.

Biography

Dr. Axel Spies
Washington, DC
+1.202.739.6145
axel.spies@morganlewis.com

Dr. Axel Spies has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and M&A. He is a co-publisher of the German Journals ZD (Journal of Data Protection) and MMR (Multimedia Law) and a co-author on two GDPR-related German handbooks.

Biography

Andrew J. Gray IV
Silicon Valley
+1.650.843.7575
andrew.gray@morganlewis.com

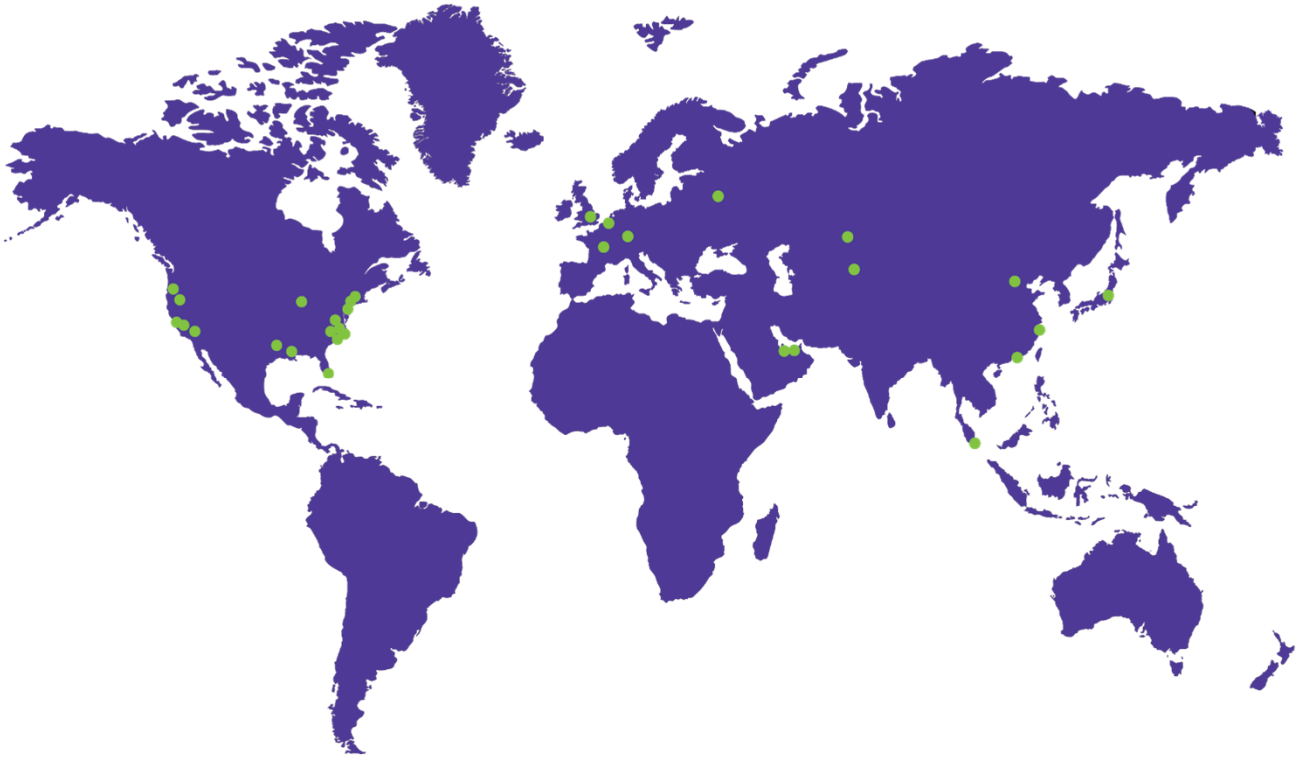
Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU