May 24, 2021

EU Privacy+Security Intensive

Jan Dhont
Wilson Sonsini, Brussels

Evie Kyriakides
Mars, Inc., London

John Bowman
Promontory, London

Privacy+ Security Forum

Speaker

Privacy+ Security Forum

Jan Dhont

Partner, Wilson Sonsini Goodrich & Rosati

Privacy and Cybersecurity

Counseling on privacy and cybersecurity matters for more than 20 years with substantive experience in working with global and U.S.-based public and private companies in a wide variety of industries. A frequent speaker on topics relating to privacy and is widely known in data privacy and security circles.

Speaker

Privacy+ Security Forum

Evie Kyriakides

Chief Data Protection & Chief Privacy Officer/ Associate General Counsel, Global Digital, Privacy & Security

Mars, Inc.

Chief Data Protection & Chief Privacy Officer/Global Digital AGC of Mars, Incorporated, has responsibility for the creation, deployment and management of global legal strategies and policies, including GDPR, in the areas of data privacy, data protection, data breaches and digital media across businesses.

Speaker

Privacy+ Security Forum

John Bowman

Senior Principal, Promontory, an IBM Company

Privacy and data protection consultant since 2014. Previously Head of EU and International Data Protection Policy at UK Ministry of Justice. In that role was Head of Delegation and Lead Negotiator for UK Government on GDPR, Law of Enforcement Directive and Convention 108.

Agenda & Timetable

Brussels, Belgium (CEST)	London, UK (BST)	Washington, DC (EDT)	Chicago, IL (CDT)	Denver, CO (MDT)	San Francisco, CA (PDT)
16:00 – 18:30	15:00 – 17:30	10:00 – 12:30	09:00 – 11:30	08:00 – 10:30	07:00 – 09:30

1. **Data Transfers Post-Schrems II**
   - Assessment of the EDPB Recommendations on data transfers
   - The new Standard Contractual Clauses
   - Relying on derogations to transfer personal information
2. **New Issues for 2021 and Beyond**
   - Brexit state of play
   - ePrivacy Regulation update
   - EU legislative developments
3. **New EDPB Guidance**
   - Data breach notification guidance
4. **Practical Exercises**
   - Data breach cases

Session 1: Data Transfers Post-Schrems II

- Assessment of the EDPB Recommendations on data transfers
- The new Standard Contractual Clauses
- Relying on derogations to transfer personal information

Privacy+ Security Forum

Introduction and Background

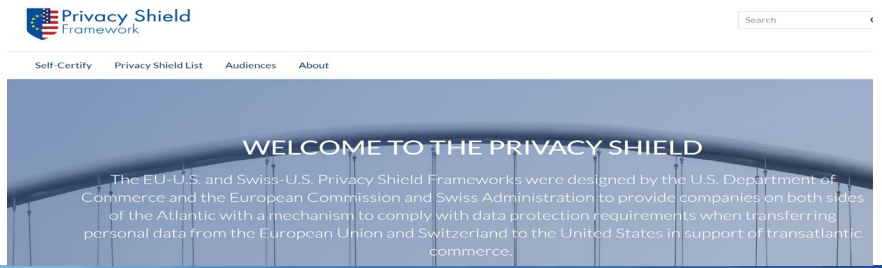
Privacy+ Security Forum

The ECJ invalidates the Privacy Shield

- Privacy Shield does not offer measures that can be deemed "essentially equivalent" to those required under EU law. Specifically:
  - FISA S. 702/EO 12333 do not provide for any limitations on the power conferred on the U.S. authorities
  - FISA S. 702/EO 12333 do not offer effective remedies to EU data subjects to challenge disclosures to U.S. authorities
- The Ombudsperson created to address complaints by EU citizens deemed to lack independence and authority to adopt decisions that bind US intelligence services

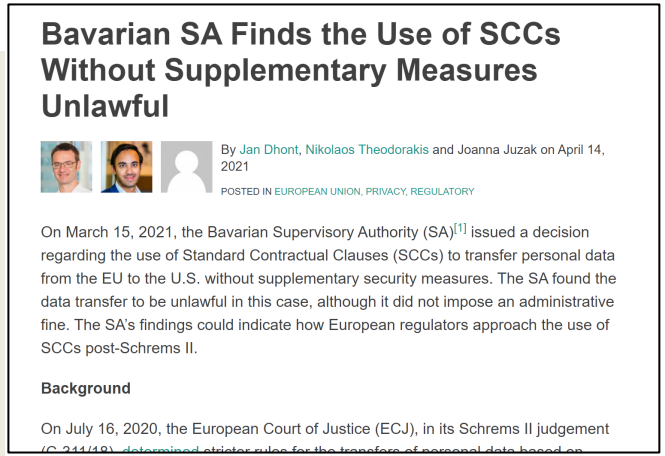
The SCCs Remain Valid

- Additional due diligence for data exporter/importer:
  - Is compliance with the SCCs possible in light of possible access by public authorities?
  - Suspend data transfers/terminate SCCs if compliance is not possible
- Affects global data transfers (US, China, India, Russia, etc.)



What Happened Since Schrems II?

- Privacy Shield companies have started switching to SCCs
- “Schrems II” Questionnaires and supplemental measures
- Legal uncertainty
  - Which companies fall under FISA702/EO12333?
  - What about transfers to countries other than the US?
  - What action is required and what type of “supplemental measures” should be required from data importers?
  - How to deal with lack of flexibility offered by the Privacy Shield (data collection from EU consumers, P-to-P and P-to-C, etc.)?
  - Are “supplemental measures” required when using BCRs?
  - Does it make sense to keep the Privacy Shield certification?
- Companies are increasingly exposed to risk and lawsuits



Bavarian SA Finds the Use of SCCs Without Supplementary Measures Unlawful

By Jan Dhont, Nikolaos Theodorakis and Joanna Juzak on April 14, 2021

POSTED IN EUROPEAN UNION, PRIVACY, REGULATORY

On March 15, 2021, the Bavarian Supervisory Authority (SA)[1] issued a decision regarding the use of Standard Contractual Clauses (SCCs) to transfer personal data from the EU to the U.S. without supplementary security measures. The SA found the data transfer to be unlawful in this case, although it did not impose an administrative fine. The SA's findings could indicate how European regulators approach the use of SCCs post-Schrems II.

Background

On July 16, 2020, the European Court of Justice (ECJ), in its Schrems II judgement

EDPB Recommendations

- Roadmap to be followed when transferring personal data outside the EU (“Transfer Tool Recommendations”)
- Examples of supplemental measures

- Guidance on how to assess a third country’s surveillance measures when exporting personal data (“European Essential Guarantees (EEG)”)

EDPB Data Transfer Methodology

Privacy+ Security Forum

- Methodology applies to all EU data exports – Matter of accountability
- Data importers outside of the EU are also affected
  - Strategize on ensuring continuity of data imports
  - May require offering some level of comfort to data exporters

Step 1 – Know Your Transfers

- Map all transfers of data leaving the EEA
  - Also include onward transfers
  - Can be challenging exercise
    - Cloud context / multiple sub-processors / access to data = data transfer / data processors and locations may change
    - Article 30 Records
  - Primarily data exporter obligation
    - However, data importers will receive questions on onward transfers from EU business partners
    - Applies to both controllers and processors

Step 2 - Identify the Relevant Data Export Mechanism

1. **Is country of import white-listed?** (Art. 45)
   Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay

No Further Action Required

2. **Appropriate Safeguards ?** (Art. 46)
   - BCRs
   - EC Standard Contractual Clauses
   - National Standard Contractual Clauses
   - Codes of Conduct
   - Certification
   - Ad hoc Contract

Further Action Required

3. **Derogations?** (Art. 49)
   - Consent
   - Performance of contract
   - Important reasons of public interest
   - Legal claims
   - Vital interests
   - Legitimate interest + notification

No Further Action Required

Step 3 - Transfer Risk Assessment

Step 3 - Transfer Risk Assessment

Elements to assess in a TRA

4 legal requirements for an interference to be acceptable:

1. Processing should be based on clear, precise and accessible rules
2. Interferences must be necessary and proportional to their objective
3. Independent oversight
4. Effective remedies for individuals whose data is transferred

Step 3 - Risk Based Approach (?)

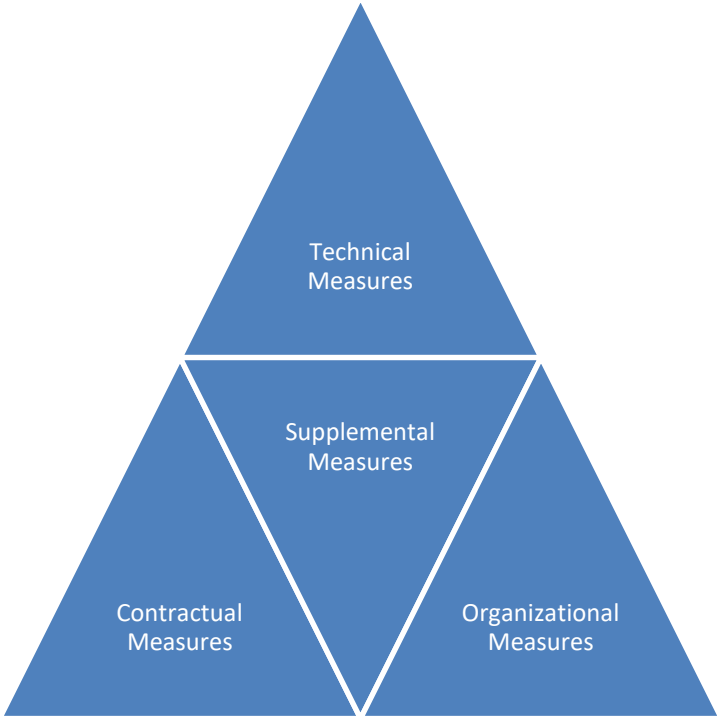
New SCCs subscribes to risk-based approach

"[T]ake into account "any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred" (New SCCs, Recital 20/Clause 2(b)(i))

Not favoured by EDPB

EDPB: "[…] you should look into […] relevant and objective factors, and not rely on subjective factors such as the likelihood of public authorities' access […]"

Step 4 – Identify and Apply Appropriate Supplementary Measures



"Contractual and organizational measures alone will generally not overcome access to personal data by public authorities of a third country"
"there will be situations where only technical measures might impede or render ineffective access by public authorities (EDPB Recommendation 01/2020, para 48)

Technical Measures

Encryption at rest and encryption in transit

- EDPB requires absolute prevention of access by government agencies "state of the art encryption" "flawlessly implemented" "resistant to crypto-analysis"
- Client-side encryption with key stored in the EU

Pseudonymization

- Effective pseudonymization is considered effective supplemental measure
- Need to ensure that re-identification is impossible

Contractual Measures

- No backdoors that allow access to personal data
- Publication of transparency reports and other information on access by public authorities
- Power to audit, obtain certifications
- Notify exporter in case of non-compliance/ access by authorities
- Warrant Canary
- Obligation to review the legality of access requests and challenge under local law
- Notify requesting authority about incompatibility of disclosure order with the transfer tool/contractual obligations
- Assist data subjects to exercise their rights
- Inform about any onward transfers / commitment not to onward transfer if equivalent protection cannot be ensured

Organizational Measures

- Internal policies with clear responsibilities for data transfers and reporting channels
- Process to review the legality of any government request and try to challenge or block any disclosure, or provide minimum information possible
- Documentation of every data access request / publication of transparency reports
- Timely involvement of the DPO or Privacy Department

Step 5 - Implement the Measures

- **SCCs:**
  - No need to request authorization from Supervisory Authority
  - Supervisory Authorities can review supplementary measures where required

- **BCRs:**
  - Schrems II reasoning applies since third countries' laws can affect protection provided to data
  - Precise impact still under discussion and specific EDPB guidance is expected

Step 6 - Periodically Re-Evaluate Safeguards

- **Monitor developments in third countries on an ongoing basis**
- **Accountability is a "continuing obligation“**
- **Mechanisms in place to suspend/end transfers where:**
  - Data importer has breached/cannot comply with commitments
  - Supplementary measures are no longer effective in third country

Market Practices and Concerns

- **Data importers:**
  - Try to accommodate clients by assessing risk to potential disclosure of data and offering supplemental measures
  - Involve vendors in assessment
- **Data exporters:**
  - Require data importers to adopt and comply with supplemental measures
  - Conduct Transfer Risk Assessments
- **In practice, risk-balancing approach that considers:**
  - The sensitivity of the information transferred (e.g. data for operational purposes, quality assurance, security etc.)
  - The likelihood that a public authority would be interested in accessing the data based on the type of business and type of data
  - Any previous access requests

Session 1: Data Transfers Post-Schrems II

- The New Standard Contractual Clauses

Privacy+ Security Forum

What Do The New SCCs Look Like?

Privacy+ Security Forum

(d) These Clauses apply with respect to the transfer of personal data as specified in Clause 5 of Section I [*Description of the Transfer(s)*].

(e) Annexes I, II and III form an integral part of these Clauses.

Clause 2

Third party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third party beneficiaries, against the data exporter and / or data importer, with the following exceptions:

(i) Section I;

(ii) Section II - Module One: Clause 1.5 (d) and Clause 1.9(b); Module Two: Clause 1.9(a), (c), (d) and (e); Module Three: Clause 1.1 and Clause 1.9(a), (c), (d) and (e); Module Four: Clause 1.1, Clause 1.2 and Clause 1.3;

(iii) Section II, Clause 3.1 (c), (d) and (e);

(iv) Section II, Clause 4;

(v) Section II - Module One: Clause 7(a), (b); Modules Two and Three: Clause 7(a), (b);

(vi) Section II, Clause 8;

(vii) Section II, Clause 9;

(viii) Section III, Clause 1 and Clause 3(a), (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 4

Hierarchy

In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Description of the transfer(s)

processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing.

1.3 Documentation and compliance

The Parties shall be able to demonstrate compliance with these Clauses.

Clause 2

Local laws affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.

(b) The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;

(ii) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;

(iii) any safeguards in addition to those under these Clauses, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph b), it has made best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

EN 13 EN

- Detailed and complex, but cover C2C, C2P, P2P and P2C
  - **Section 1**: General – Scope, third party beneficiary rights, interpretation, hierarchy, description of transfer, docking clause
  - **Section 2**: Modular – Obligations of the parties
  - **Section 3**: Final provisions – non-compliance, termination, governing law, forum
  - **Annexes** : List of parties, description of transfers, technical and organizational measures, list of sub-processors
- Different obligations depending on scenario
- Long awaited scenarios: non-EEA transfers, P2P and P2C

Main Proposed Novelties for Data Importers (1/2)

More Detailed Notice Requirements

- **C2C:** Identity and contact details of importer, further processing for different purpose by importer, and onward transfers (also potentially categories of data processed, data retention)

Data Breach Notification Requirements

- **C2C:** Notify data breaches both to the data exporter and the "competent supervisory authority" and data subjects (if "high risk")
- **C2P:** Notify data exporter
- **P2P:** Notify data exporter and controller (if appropriate)

Tight(er) Onward Transfer Requirements

- **C2C:** Data importer must provide equivalent protection in all cases, also if onward transfer to data processor
- **C2P/P2P:** Ensure "equivalent protection" (in practice: importer in white-listed country; importer becomes party to SCCs; SCCs with data exporter; transferee is bound by BCRs)

Main Proposed Novelties for Data Importers (2/2)

Accountability Requirements

- Importer must keep "appropriate documentation" available to the "competent supervisory authority" (all 4 modules)
- Keep documentation available to exporter (C2P) and controller (P2P)

Liability

- Importer is jointly and severally liable to data subjects together with exporter, if both are responsible for damage

"Schrems II Provisions"

- Reps and warranties
  - "No reason to believe" law impinges on protection of the SCCs / "best effort" cooperation with exporter by providing relevant information to conduct TIA / will cooperate with exporter in ensuring compliance with the SCCs
  - Representation to notify exporter if law changes that may adversely affect level of protection

Government access requests

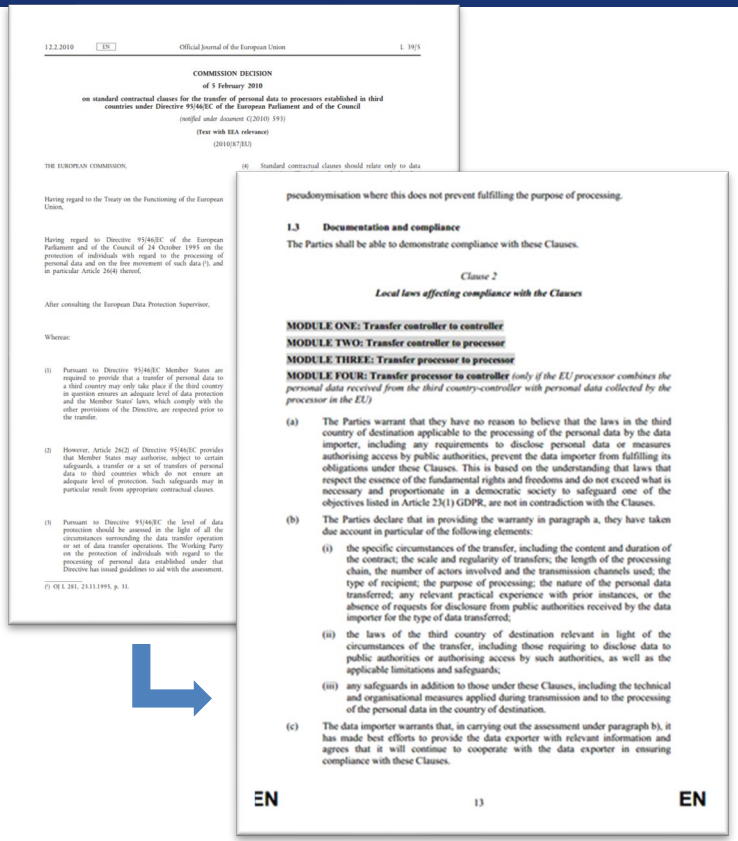
- Notify exporter and (where possible) data subject of government access requests
- Assess legality under its local laws and challenge request / document assessment
- Apply data minimization when responding to request
- Provide exporter and “competent supervisory authority” with transparency reports on received access requests

Main Novelties for Data Exporters

- **Determine Extent of Obligations**
  - **Relationship between importer and exporter will determine exporter's obligations:**
    - P2P transfers: exporter must inform importer that exporter is a processor and **provide information on controller(s) to importer** prior to processing
    - P2P transfers: exporter must **forward importer's notifications** regarding government access requests to data controller
    - C2C transfers: importers are required to **provide a prescriptive list of information to data subjects**; in practice, such information will most likely be provided through exporter's privacy policy

- **"Schrems II Provisions"**
  - Make **TIA documentation** available to SA upon request
  - **Exporters must identify supplementary measures** if (i) exporter has reasons to believe importer cannot fulfil its obligations under the clauses/lack of equivalent protection, or (ii) importer notifies the exporter that laws of importing country prevent it from fulfilling its obligations under SCCs. **Notification to SA** if exporter continues transfers **with supplementary measures**

New SCCs



12.2.2010 EN Official Journal of the European Union L 39/5

COMMISSION DECISION

of 5 February 2010

on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

(notified under document C(2010) 593)

(Text with EEA relevance)

(2010/87/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1), and in particular Article 26(4) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on the protection of individuals with regard to the processing of personal data established under that Directive has issued guidelines to aid with the assessment.

(1) OJ L 281, 23.11.1995, p. 31.

(4) Standard contractual clauses should relate only to data

pseudonymisation where this does not prevent fulfilling the purpose of processing.

1.3 Documentation and compliance

The Parties shall be able to demonstrate compliance with these Clauses.

Clause 2

Local laws affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.

(b) The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;

(ii) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;

(iii) any safeguards in addition to those under these Clauses, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph b), it has made best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

EN 13 EN

- **Existing SCCs in place?**
  - Draft SCCs foresee a one-year transition period during which transfers may continue on the basis of the current SCCs
  - However, if changes are required to those SCCs during that period, parties must already switch to the new SCCs
- **How to implement the SCCs in practice?**
  - Implementation process will be broadly the same as for the current SCCs, adapted for the modular nature of the new SCCs
  - Start from the framework provisions
  - Select the applicable module
  - Sign as a standalone contract or include into existing contracts
  - Have additional parties sign up (where applicable)

Session 1: Data Transfers Post-Schrems II

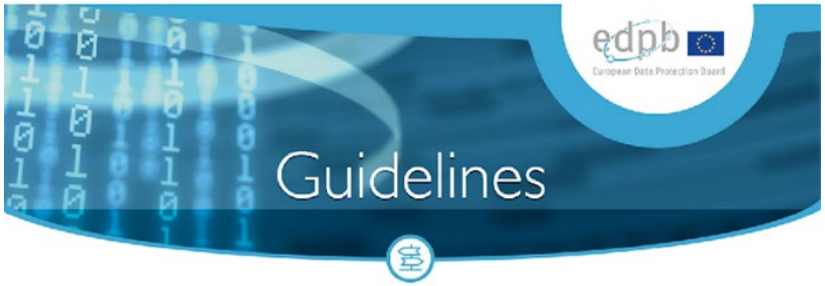
- Relying on Derogations to Transfer Personal Information

Privacy+ Security Forum

Derogations – A Reliable Ground To Transfer Data?

- EDPB: “Derogations must be interpreted restrictively so that the exception does not become the rule” (“Derogations for specific situations”)

- EDPB: “Transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned”



Derogations – A Reliable Ground To Transfer Data?

- *ECJ Schrems II Ruling*: "[…] the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR." (Para 202).

- "[…] In my opinion, the opportunities granted by Article 49 have not been fully explored yet. I believe they are not so narrow that they restrict any kind of transfer, especially when we're talking about transfers within one corporation or group of companies" - *ECJ Judge von Danwitz*

Derogations - General Requirements

- **Occasional and Non-Repetitive Transfers**
  - Not for regular data transfers
  - Outside the regular course of actions
  - Not in case of direct access to an information system

Explicit Consent

- Consent must be freely given, specific, informed and unambiguous (WP 259)
- Additional conditions
  - Consent must be **explicit**
  - Consent must be **specific** for the particular transfer/set of transfers
  - Consent must be **informed** particularly as to the "possible risks of [the] transfer"
    - **Specific circumstances** of the transfer (i.e. the data controller's identity, the purposes of the transfer, the type of data, the existence of the right to withdraw consent, the identity or the categories or recipients)
    - **Specific risks** as country of import does not provide for adequate data protection, and no safeguards are implemented to protect the data post transfer (e.g. no Supervisory Authority, no data privacy rights post-transfer,…)
    - Specify all data recipients or **categories of recipients**, all **countries** to which the personal data are being transferred to and confirm that consent is lawful ground for the transfer
- Consent must be withdrawable anytime

Contract Performance

A. Between the Data Subject and the controller / implementation of precontractual measures taken at the data subject's request

- **Necessity test**
  - Need for a sufficiently close and substantial connection between the data transfer and the purposes of the contract
    - E.g. Travel agents transferring data for booking purposes to hotel or other commercial partners
    - Not: for transfer of additional information not necessary for performance of the contract
    - Not: centralized payment and human resources management functions

- **Only for occasional transfers**
  - E.g. payment data transferred to a bank in a third country to execute a payment request
    - Not: data transfers regularly occurring within a stable relationship (typically data transfers within a business relationship)

Contract Performance

B. Contract concluded in the interest of the data subject between the controller and another natural or legal person

- Necessity of the data transfer and conclusion of the contract in the interest of the data subject
  - Not in case of outsourced data processing (e.g. payment processing in favor of employee)
  - A close relationship must be established between the transfer and a contract concluded in the data subject's interest

- Occasional transfers only

Transfer is Necessary for the Establishment, Exercise or Defense of Legal Claims

- **Regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies**
  - E.g. for purpose of defense or to obtain a reduction or waiver of a fine in criminal or administrative proceedings (e.g. antitrust, corruption, insider trading or similar procedures)
  - E.g. data transfers for the purpose of pre-trial discovery procedures
  - E.g. actions by the data exporter to institute procedures in a third country (e.g. commencing litigation in a third country)
  - Also “out-of-court” procedures or for purposes of “seeking approval for a merger”
  - Not: if legal proceedings are hypothetical / may be brought in the future
- **Occasional transfers only**
- **Close link between data transfer and a specific procedure**
  - Data must be necessary in a specific procedure
  - Data minimization and anonymization / de-identification / redaction where possible

Transfer Necessary to Protect the Vital Interests of the Data Subject or Other Persons

- **Vital interest**
  - E.g., medical emergency situations
  - Not for situations outside medical treatment, such as general medical research
  - Can be relied on to protect both the physical and mental integrity

- **Necessity test**
  - The data must be necessary for an essential diagnosis

- **Data subject is not physically or legally capable to provide consent**
  - For instance, in case of natural disasters for purposes of rescue and retrieval operations

Compelling Legitimate Interests

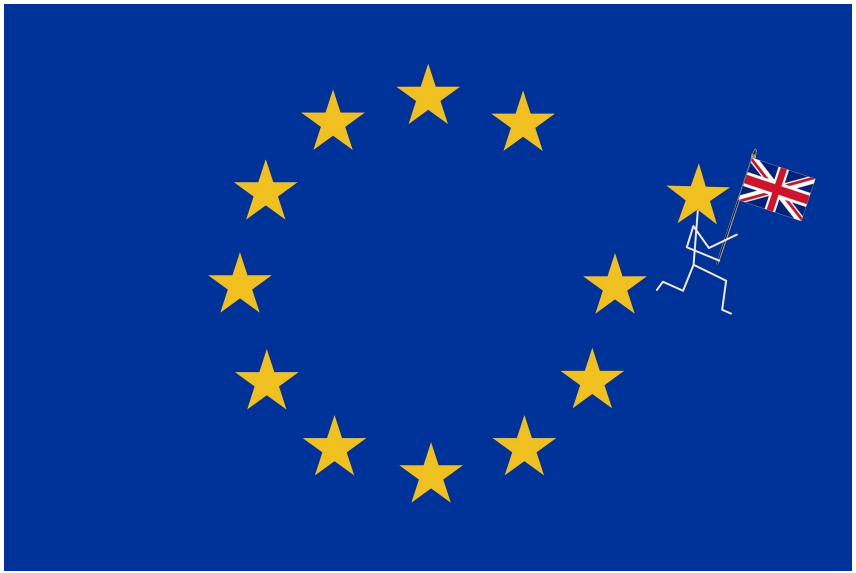
- **Last resort derogation**
  - Data exporter must be able to demonstrate that it was not possible to rely on Article 45 and 46 GDPR or any of the other Article 49 GDPR derogations
- **Compelling legitimate interests of the controller**
  - E.g. "*if a data controller is compelled to transfer personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business*"
  - Need to be conveyed to the data subject
- **Non-repetitive transfers only**
- **Limited number of data subjects**
- **Balancing test of legitimate interests v. rights and freedoms of data subjects**
  - Possible negative effects / likelihood and severity of risks / potential damage
  - Nature of the data / purpose and duration of the processing / situation in country of destination
  - Apply additional safeguards (e.g. deletion of data as soon as possible, limited processing purposes, encryption or pseudonymization)
- **Notification of the Supervisory Authority**
- **Information to data subject about compelling legitimate interests pursued**

Session 2: New Issues for 2021 and Beyond

- Brexit State of Play
- ePrivacy Regulation update
- EU legislative developments

Privacy+ Security Forum

UK Leaves the EU



- UK left EU on 31 Jan 2020
- No participation in EU institutions (European Council, European Parliament etc.)
- UK ICO no longer participates in EDPB

Brexit Transition Period

- Brexit transition period from 1 Feb 2020 to 31 Dec 2020
- Provided for continuity of rules
- Free flow of personal data between EU-UK maintained

End of Transition Period

- EU-UK Trade & Cooperation Agreement agreed on 24 Dec 2020
- Interim provision for transmission of personal data to UK, until 30 Apr 2021, extendable to 30 Jun 2021

European Union (Withdrawal Act

- Retained EU law
- Retained case law
- Continuity
- Exceptions

European Union (Withdrawal) Act 2018

2018 CHAPTER 16

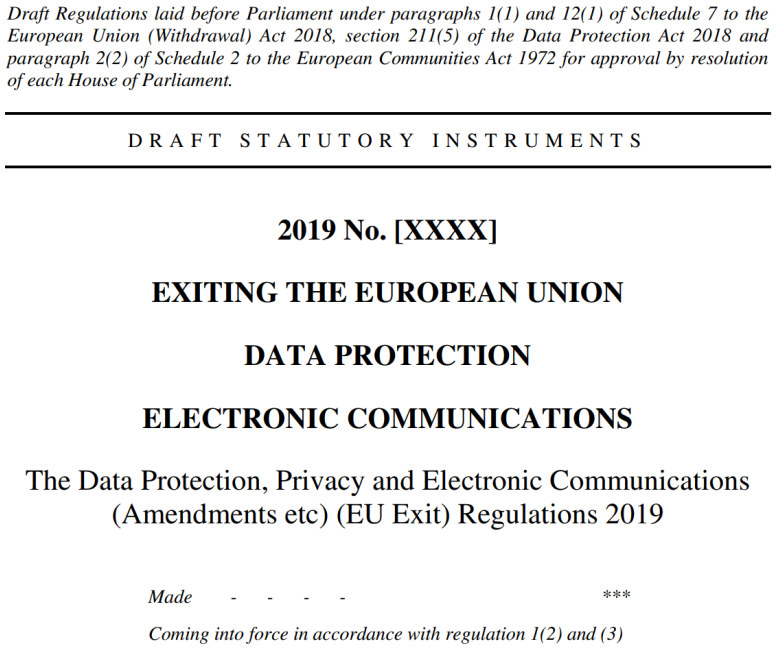
An Act to repeal the European Communities Act 1972 and make other provision in connection with the withdrawal of the United Kingdom from the EU.

[26th June 2018]

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

UK GDPR & DPA 2018

- UK GDPR sits alongside DPA 2018
- Same text as EU GDPR but some technical changes made (EU references removed)
- Article 48 omitted from UK GDPR
- DPA 2018 also cover LED and national security processing under C108



Draft Regulations laid before Parliament under paragraphs 1(1) and 12(1) of Schedule 7 to the European Union (Withdrawal) Act 2018, section 211(5) of the Data Protection Act 2018 and paragraph 2(2) of Schedule 2 to the European Communities Act 1972 for approval by resolution of each House of Parliament.

DRAFT STATUTORY INSTRUMENTS

2019 No. [XXXX]

EXITING THE EUROPEAN UNION

DATA PROTECTION

ELECTRONIC COMMUNICATIONS

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Made - - - - ***

Coming into force in accordance with regulation 1(2) and (3)

Adequacy for the UK?

EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom

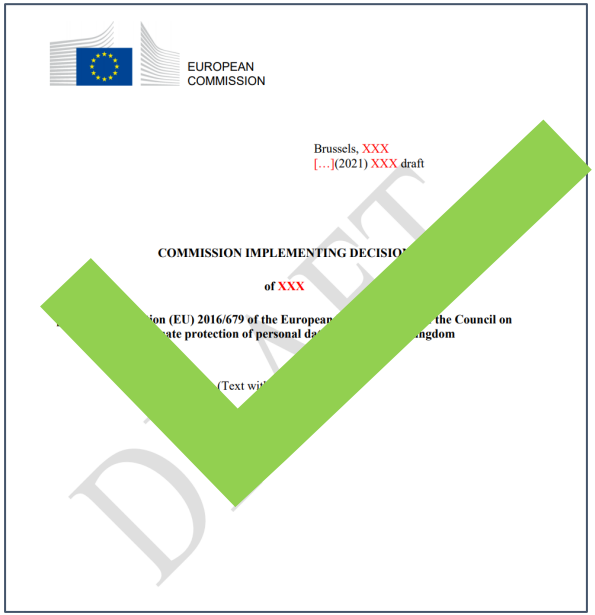
(Text with EEA relevance)

DRAFT

- Two draft adequacy decisions published (GDPR & LED) 21 Feb 2021
- EDPB published opinion on draft decisions 16 April 2021
- European Parliament resolutions May 2021
- Final approval needed by Council of EU and College of Commissioners by 30 June

What if Adequacy is granted?

- EU to UK data transfers maintained
- No additional data transfer mechanisms required

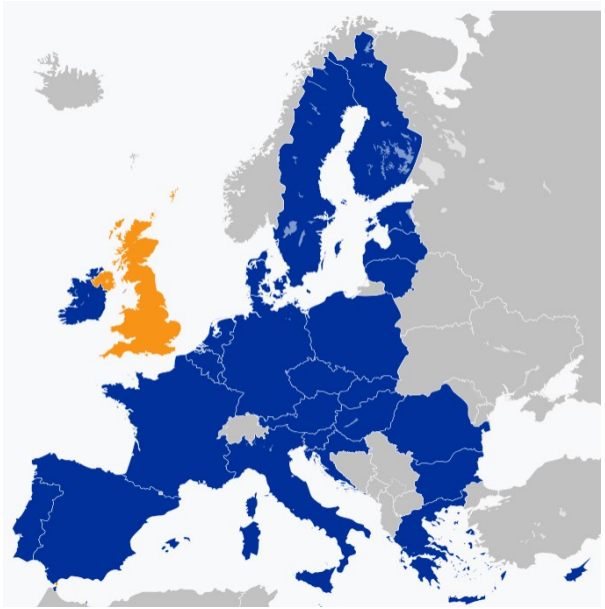


What if Adequacy is not granted?

- GDPR data transfer mechanisms need to be applied for EU to UK flows
- Schrems II-compliant measures need to be applied

Exporting data from the UK

- Transfers to EU/EEA can continue
- Existing EU adequacy decisions are recognised
- SCCs and BCRs remain valid for 3rd countries but may need amendment



Engaging with Regulators

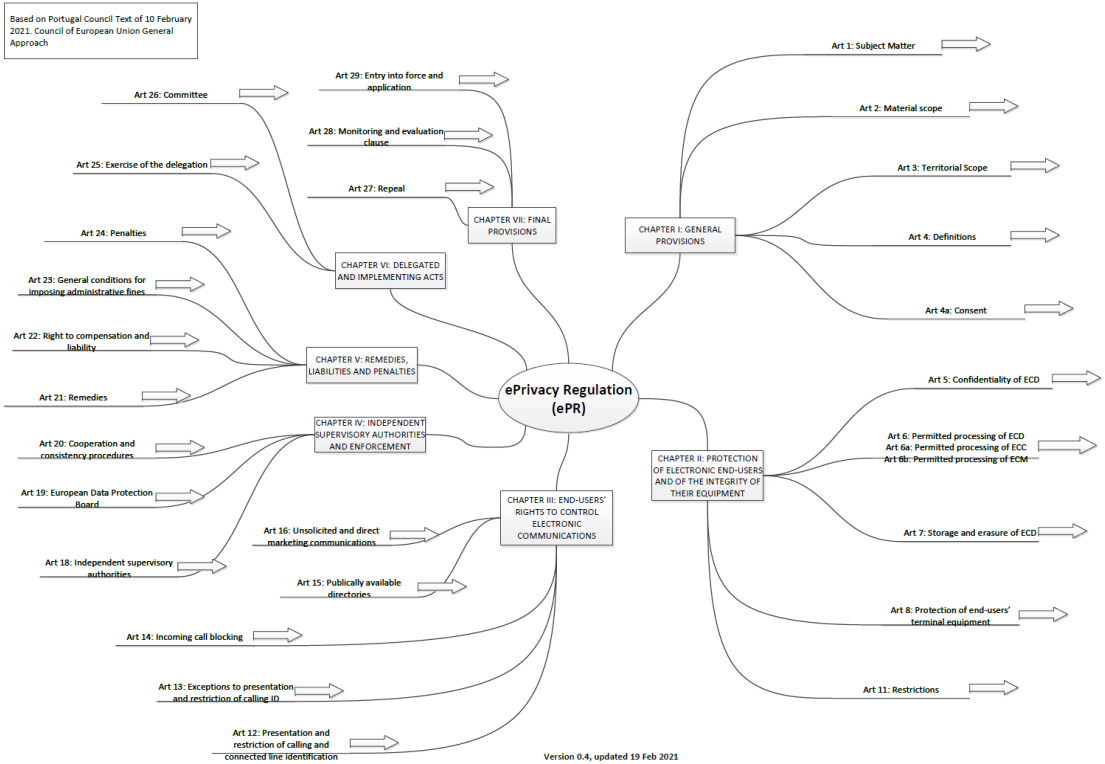
- UK data controllers: may need new main establishment or representative in EU
- EU data controllers: may need an establishment or representative in the UK
- UK BCR holders: will need a new BCR Lead Supervisory Authority in EU

Challenges and opportunities

- Divergence of rules: less GDPR harmonisation but lower burdens on business?
- Can UK maintain a high level of data protection outside of EU?
- UK National Data Strategy (NDS) “is an ambitious, pro-growth strategy that drives the UK in building a world-leading data economy while ensuring public trust in data use.”
- ICO/CMA* – intersection of data protection and competition law. Update MoU agreed.
- “The ICO and the CMA are already collaborating on a number projects, including the ICO's ongoing investigation into adtech and real-time bidding.”

**Competition and Markets Authority*

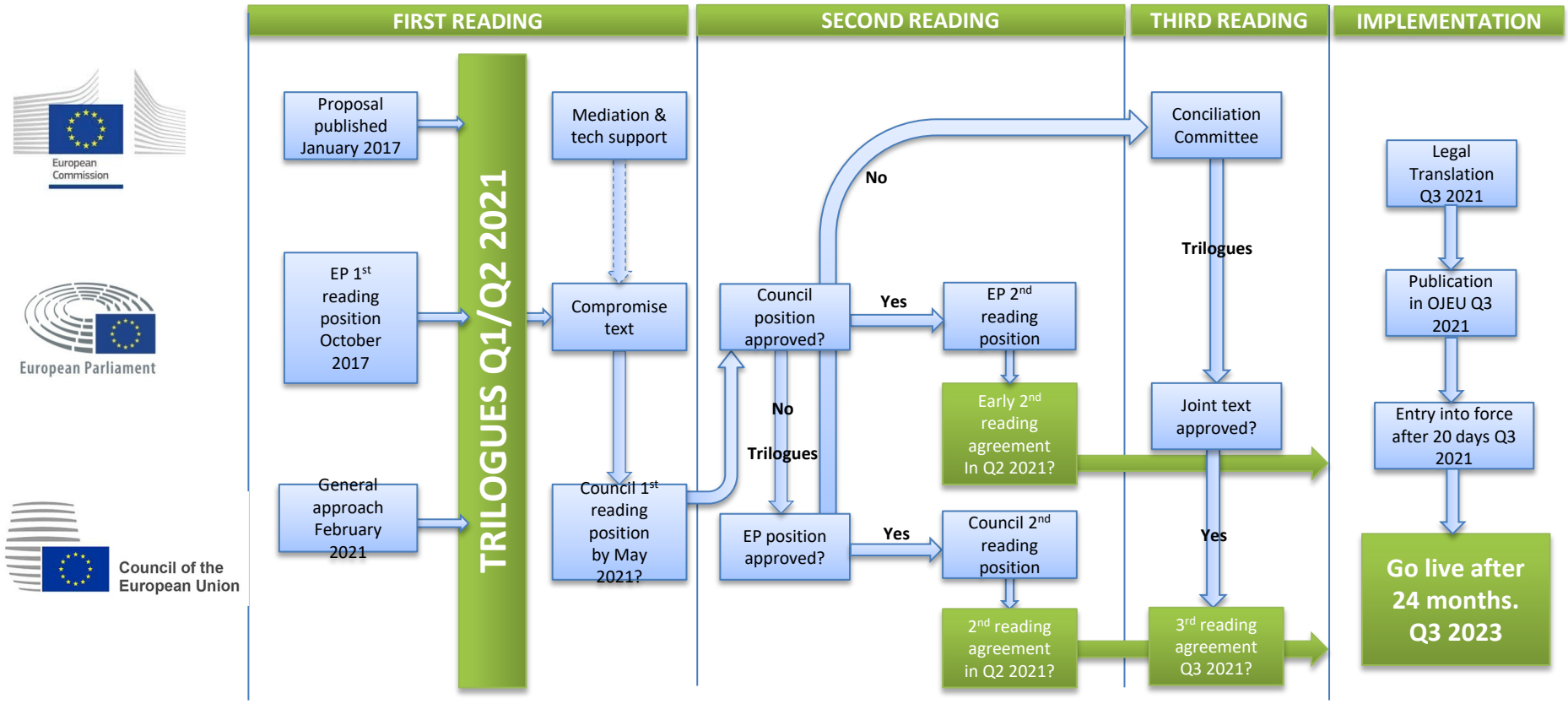
ePrivacy Regulation update



Main features of ePR

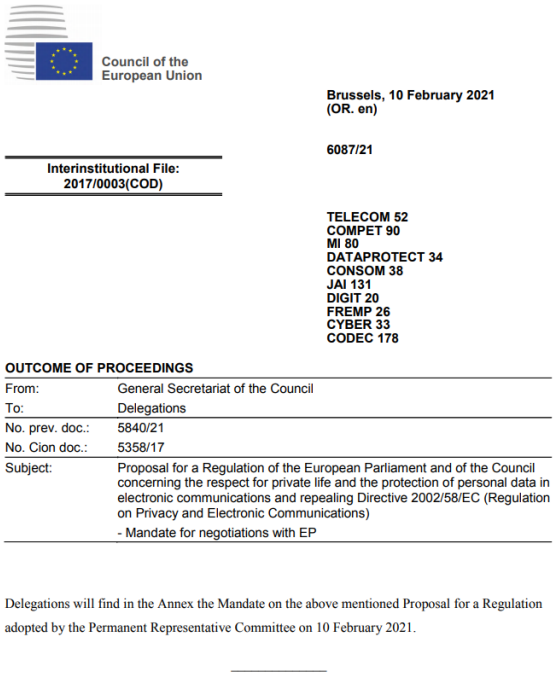
- The proposed ePrivacy Regulation (ePR) lays down rules regarding respect for private life and communications. It protects communications of natural and legal persons
- ePR complements the GDPR and replaces the current ePrivacy Directive from 2002 (amended in 2009)
- Sets requirements for electronic communications, cookies, direct marketing and connected devices
- Strong emphasis on consent to process communications data and for information to be erased or anonymised following transmission
- Personal data and non-personal data are within scope of ePR
- Enhanced enforcement powers and increased fines of up to 20million EUR or 4% of annual global turnover (as per GDPR)

Path to agreement



Council Draft Text – Feb 2021 (1)

- The regulation will cover electronic communications **content** transmitted using publicly available services and networks, and **metadata** related to the communication.
- The rules will also cover machine-to-machine data transmitted via a public network (**Internet of Things**)
- The rules will apply when **end-users** are **in the EU**.
- As a main rule, **electronic communications data** will be **confidential**.
- **Permitted processing** of electronic communications data without the consent of the user includes, for example, ensuring the integrity of communications, or to prevent crime or threats to public security.
- **Metadata** may be processed for instance for billing, or for detecting or stopping fraudulent use. **With the user's consent**, service providers could, use metadata to display traffic movements.



Council of the European Union

Brussels, 10 February 2021
(OR. en)

6087/21

Interinstitutional File:
2017/0003(COD)

TELECOM 52
COMPET 90
MI 80
DATAPROTECT 34
CONSOM 38
JAI 131
DIGIT 20
FREMP 26
CYBER 33
CODEC 178

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	5840/21
No. Cion doc.:	5358/17
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP

Delegations will find in the Annex the Mandate on the above mentioned Proposal for a Regulation adopted by the Permanent Representative Committee on 10 February 2021.

Council Draft Text – Feb 2021 (2)

- Providers of electronic communications networks and services **may process metadata** for a purpose other than that for which it was collected, even when this is not based on the user's consent. This processing for another purpose must be **compatible** with the initial purpose
- As the user's **terminal equipment** may store highly personal information, such as photos and contact lists, the use of processing and storage capabilities and the collection of information from the device will only be allowed with the **user's consent** or for other specific transparent purposes
- The end-user should have a **genuine choice** on whether to accept **cookies** or similar identifiers..
- To avoid **cookie consent fatigue**, an end-user will be able to give consent to the use of certain types of cookies by whitelisting one or several providers in their browser settings.

Council of the European Union

EDPB Statement on ePR – Mar 2021 (1)

- **ePR must under no circumstances lower the level of protection** offered by the current ePrivacy Directive but should complement the GDPR by providing additional strong guarantees for confidentiality and protection of all types of electronic communication
- This **right to confidentiality must be applied to every electronic communication,** regardless of the means by which they are sent, at rest and in transit, from the sender to the receiver, and must also protect the integrity of every user's terminal equipment.
- The EDPB is **concerned that some exceptions** (in particular access to communications data and content to ensure network and end-user device security) introduced by the Council **seem to allow for very broad types of processing**
- Allowing the access of electronic communications data, including content, to ensure network and end user device security **could allow full access** by the electronic communication service provider or their processors **to the contents of all end user communications.**

Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications

The Data Protection Authorities of the European Union, united in the European Data Protection Board, consider that the revision of the current ePrivacy Directive (2002/58/EC, amended by 2009/136/EC) is an important and necessary step that has to be concluded rapidly. The use of IP based communication services has become widespread since 2009, and these 'Over-the-Top' services are currently not covered by the existing Directive; in order to ensure that end-users' confidentiality of communications is protected while using these new services and to create a level playing field for providers of electronic communication and functionally equivalent services, we call on the European Commission, Parliament and Council to work together to ensure a swift adoption of the new ePrivacy Regulation, replacing the current Directive as soon as possible after the coming into effect of the General Data Protection Regulation in May this year.

Given the developments in deliberations on the proposal, and for the benefit of the co-legislators, the EDPB has decided to offer further advice and clarifications on some specific issues raised by the proposed amendments by the co-legislator.

1. Confidentiality of electronic communications requires specific protection beyond the GDPR

Confidentiality of communications (the modern equivalent of the traditional postal secrecy of correspondence) is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union, already implemented by the ePrivacy Directive. This right to confidentiality must be applied to every electronic communications, regardless of the means by which they are sent, at rest and in transit, from the sender to the receiver, and must also protect the integrity of every user's terminal equipment.

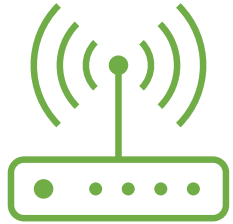
Electronic communications are the keystone of many essential activities of our modern societies, since they support the exercise of many fundamental rights such as freedom of thought, conscience, religion, expression, information, assembly, association, etc. Reinforcing the confidentiality and neutrality of the messaging services delivering our communications is therefore a necessity.

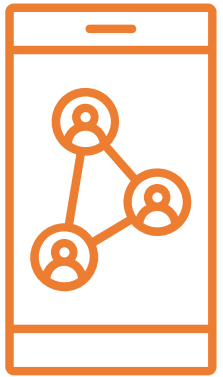
Given the importance and the widespread use of electronic communications in our digital lives, they are very likely to contain, or to reveal, special categories of personal data, either explicitly or because of mere accumulation and combination of electronic communications content or metadata, which can allow very precise conclusions concerning the private lives of the people to be drawn, implying high risks for their rights and freedoms, and should therefore be treated accordingly.

Therefore, we fully support the approach of the proposed Regulation, based on broad prohibitions, narrow exceptions, and the use of consent. Accordingly, there should be no possibility under the ePrivacy Regulation to process electronic communications content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service. Furthermore, there should be no possibility under the ePrivacy Regulation to process electronic communications metadata

EDPB Statement on ePR – Mar 2021 (2)

- **ePR should emphasize the role of anonymisation** as the core guarantee that should be systematically favoured when it comes to the use of electronic communication data.
- **Strong state-of-the-art encryption** should be the general rule to ensure a secure, free and reliable flow of data. End-to-end encryption, from the sender to the recipient, is also the only way to ensure full protection of data in transit.
- **ePR must enforce the consent requirement for cookies** and similar technologies, and offer service providers technical tools allowing them to easily obtain such consent
- ePR should improve the current situation by **giving back control to users and addressing "consent fatigue"**.
- On the **further processing** of electronic communications metadata/data collected through cookies and similar technologies, the EDPB reiterates its support for a **general prohibition**, followed by **narrow exceptions** and the **use of consent**.





Proposed EU Regulation on AI

Privacy+ Security Forum

Current international AI landscape

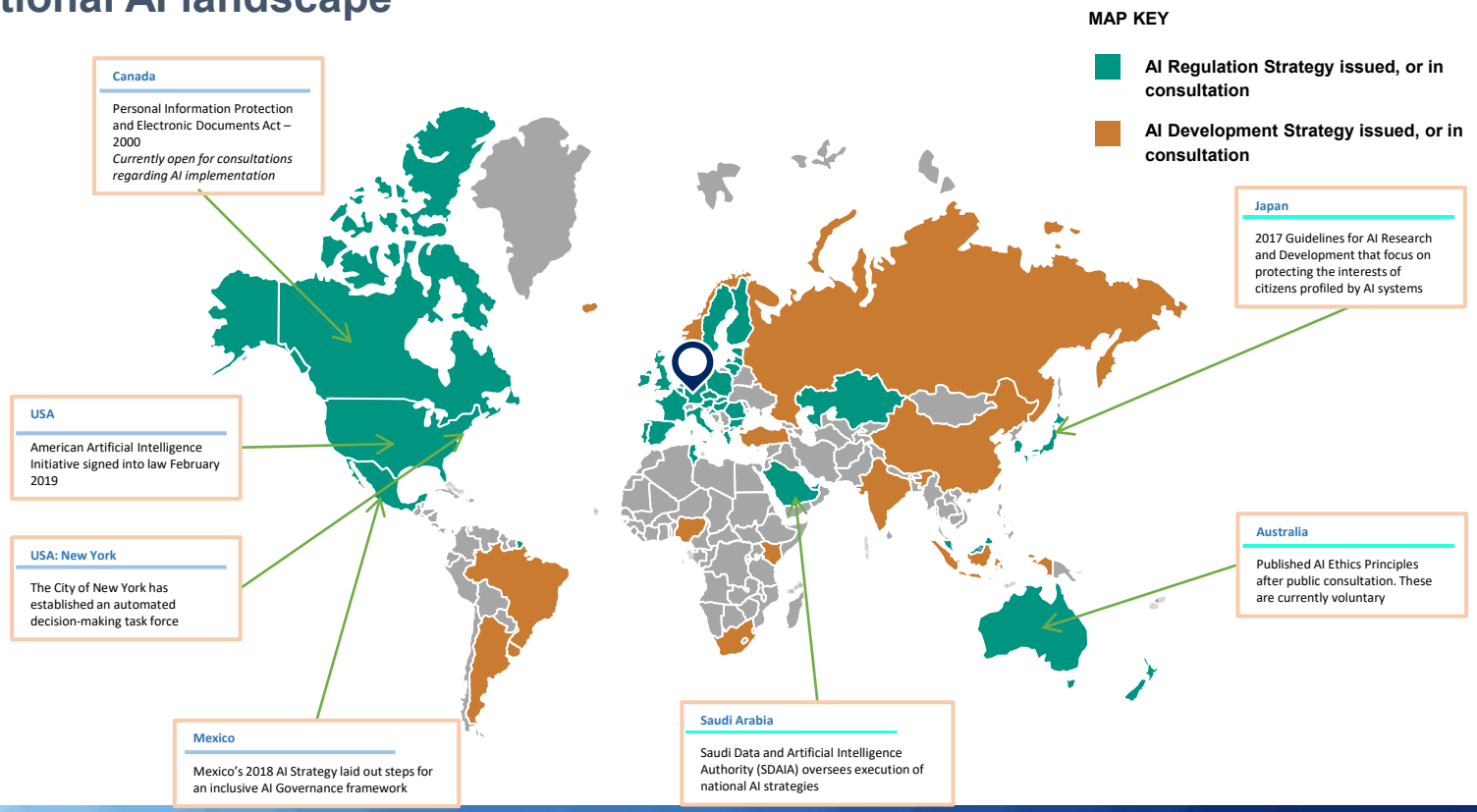
European Union

Publications

- EU Guidelines on ethics in Artificial Intelligence: Context and Implementation
- EDPB Strategy 2021-2023
- Artificial intelligence: Presidency issues conclusions on ensuring respect for fundamental rights
- Artificial intelligence: threats and opportunities

Committees and Assemblies

- Second European AI Alliance Assembly
- Special Committee on Artificial Intelligence in a Digital Age
- High-level expert group on artificial intelligence



Overview of European Commission AI Regulation proposal

The European Commission has published a proposed AI Regulation. The framework will address and offer mitigation recommendations for risks to public safety and privacy from AI systems, as well as establishing a governance structure across the EU.

Key Publication Points
- Applicable to all Member States
- Published in conjunction with a Coordinated Plan
- First Regulatory Framework Globally

Aims
- Reduce administrative and financial burdens on developers (particularly SMEs)
- Protection of citizens

Who it applies to
- All providers who offers AI services in the EEA
- All users of AI in the EEA
- Where AI outputs are utilised in the EEA

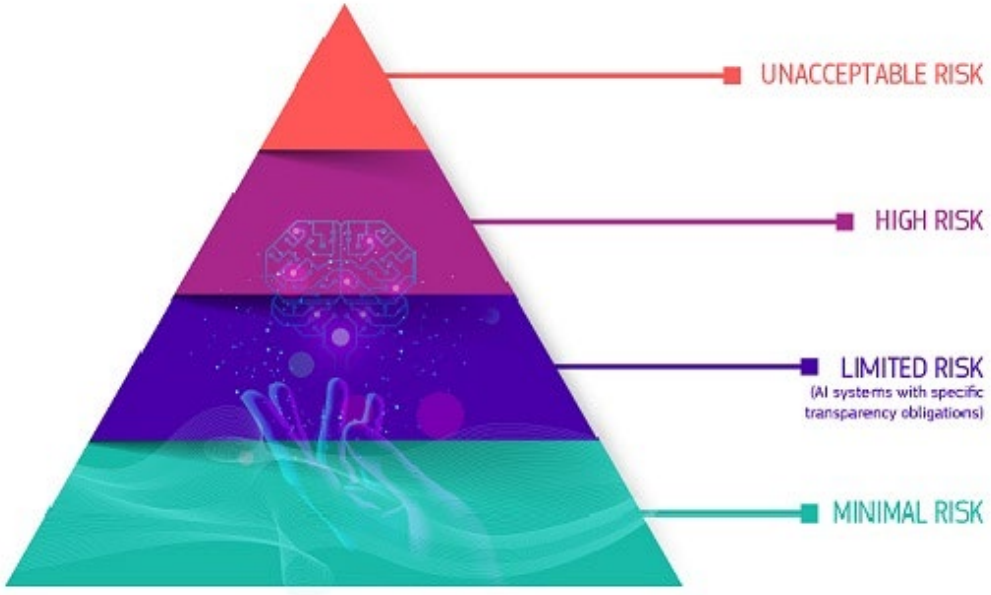
The proposed rules will:

- Address risks specifically created by AI applications
- Propose a list of high-risk applications
- Set clear requirements for AI systems for high-risk applications
- Define specific obligations for AI users and providers of high-risk applications
- Propose a conformity assessment before the AI system is put into service or placed on the market
- Propose enforcement after such an AI system is placed in the market
- Propose a governance structure at European and national level

European Commission AI Framework – Risk Review

Privacy+ Security Forum

The new framework will require all AI systems to be scored a risk rating through a conformity assessment:



- All biometric identification systems are considered high risk; their use in public spaces is prohibited unless by law enforcement for specified purposes.
- The regulations do not apply to AI used for military purposes.

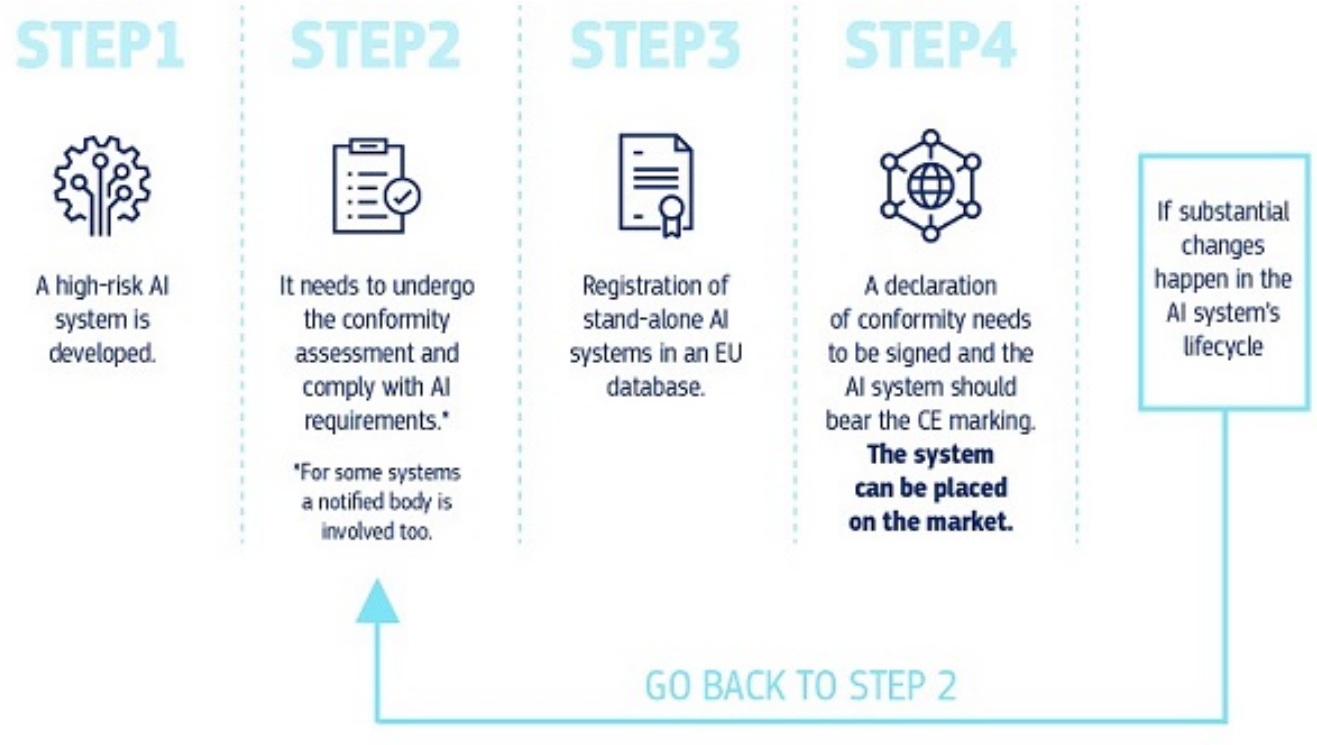
• **Unacceptable Risk;** systems which pose a clear threat to the safety, livelihoods and rights of individuals will be banned (e.g. social scoring by governments).

• **High Risk;** including systems which determine access to education (e.g. scoring of exams), essential public and private services, democratic and lawful processes, and safety components of systems that may affect the health of citizens (e.g. robot-assisted surgery). *Subject to strict obligations before being allowed to go to market.*

• **Limited Risk;** including chatbots, and similar interactive technologies. *Transparency required.*

• **Minimal Risk;** including AI-enabled video games and spam filters. *Free use allowed.*

Regulation and Enforcement



Enforcement

Enforcement and regulation will be overseen by a new European Artificial Intelligence Board (EAIB), and competent authorities to supervise compliance at a national level.

Proposed fines for non-compliance:

- **2% of annual worldwide turnover or €10 million;** for incorrect, incomplete, or misleading information to supervisory bodies or other public authorities.
- **4% of annual global turnover or €20 million;** for non-compliant AI systems.
- **6% of annual global turnover or €30 million;** for deployment of unacceptable risk systems, or violations of governance obligations.

AI Framework – privacy overlaps

Privacy+ Security Forum

- Third party obligations and contracting
- Transparency obligations
- Record keeping obligations
- Incident logs
- Human Oversight

Next steps

- The proposal is set to be reviewed and debated by the European Council and Parliament.
- The regulation is expected to enter into force in late 2022 beginning a transitional period, with enforcement expected from late 2024.

Early criticism:

- Loopholes for use of biometric identification by law enforcement.
- The “intended to be used” loophole.
- No requirement to inform people if they are subject to AI assessment.

EU Data Strategy: to create a single market for data

Privacy+ Security Forum

Existing legislation	Future initiatives
GDPR	EU Data Governance Act
Open Data Directive	EU Digital Services Act
ePrivacy Directive	EU Digital Markets Act
	ePrivacy Regulation
	EU Data Act
	EU Cybersecurity Strategy
	European Health Data Space Initiative

EU Data Governance Act: focus areas

Health data

Mobility data

Public administration data

Agricultural data

Environmental data

EU Data Governance Act: key points (1)

Privacy+ Security Forum

- **Introduces a new concept of data altruism:** its aim is to enhance the ability of consumers to manage their data and enable them to share it for the common good in acts of "data altruism". Public hospitals, for example, could share data to help tackle public health emergencies, or individuals could donate data for scientific research.
- **Introduces Intermediaries**: the proposed Act envisages the sharing of data through trusted "intermediaries", which would act as clearinghouses between businesses and individuals. These are envisaged to be new organisations, such as data unions or data cooperatives. Must be not-for-profits and legally separate.
- **Establishes a European Data Innovation Board** in the form of an Expert Group consisting of representatives of the Member States, the European Data Protection Board and representatives of relevant data spaces and specific sectors.
- **Gives natural and legal persons the right to lodge a complaint** with the relevant national competent authority against providers of data sharing services or data altruism organizations. It also provides a right to an effective judicial remedy.

EU Data Governance Act: key points (2)

Privacy+ Security Forum

- **Jurisdiction:** organisations that facilitate the sharing of data must be based in the EU.
- **Remuneration:** aims to boost the sharing of data among businesses. Data will be made available on a voluntary basis, unless required otherwise by law, and can be reused against remuneration or for free, depending on the data holder's decision.
- **Sensitive data:** a mechanism would be created to permit the reuse of public-sector data that is deemed "sensitive" because of personal data, commercial or statistical confidentiality or intellectual property rights. Public-sector bodies would be able to charge fees for the data.
- **Provides a framework for the voluntary registration** of entities that collect and process data made available for altruistic purposes, such as scientific research etc.
- **Penalties:** “Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.”

The Concept of Data Altruism

- Creates opportunities for individuals or companies **to make data voluntarily available for reuse**, without compensation, for the common good, such as for scientific research or improving public services.
- There will be a **register of organisations** that facilitate data sharing. These **organisations must be not-for-profits**.
- They will have **transparency obligations** and must be legally separate.
- European data altruism **consent form**
- The consent form shall **ensure that individuals are able to provide and withdraw consent**, for a specific data processing operation, in line with the GDPR.

EU Digital Services Act

The proposed **EU Digital Services Act** will provide a common set of rules on intermediaries' obligations and accountability across the single market while ensuring a high level of protection to all users. It aims to provide easy and clear ways to report illegal content, goods or services on online platforms, particularly related to

Key features include:

- **measures to counter illegal goods, services or content online**, such as a mechanism for users to flag such content and for platforms to cooperate with “trusted flaggers”
- **new obligations on traceability of business users** in online market places, to help identify sellers of illegal goods.
- **effective safeguards for users**, including the possibility to challenge platforms’ content moderation decisions
- **transparency measures for online platforms** on a variety of issues, including on the algorithms used for recommendations
- **obligations for very large platforms** to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems
- **access for researchers to key data** of the largest platforms, in order to understand how online risks evolve
- **oversight structure to address the complexity of the online space:** EU countries will have the primary role, supported by a new **European Board for Digital Services**; for very large platforms, enhanced supervision and enforcement by the Commission

EU Digital Markets Act

The proposed EU Digital Markets Act sits alongside the Digital Services Act/

- The DMA regulates the **behaviour of core platform services acting as gatekeepers**. Think of its purpose in terms of competition law.
- Gatekeepers are those platforms that serve as an **important gateway between business users and their customers** and enjoy a significant and durable market position.
- The Digital Markets Act imposes **several prohibitions and obligations on gatekeepers**, such as the prohibition to discriminate in favour of their own services and obligations to share data that is generated by business users and their customers in their use of the platform.
- **Sanctions**: fines of up to 10% of the company's total worldwide annual turnover and periodic penalty payments of up to 5% of the company's total worldwide annual turnover.

Session 3: New EDPB Guidance

- Data breach notification guidance

Privacy+ Security Forum

EDPB Data Breach Guidance

- Description of 6 common types of data breaches (ransomware attack, data exfiltration attacks, internal human risk, lost or stolen device and paper docs, misposted data, and social engineering attacks)

- 18 case studies

- Practical recommendations on how to assess risk

- **Recommendations**
  - Notify SA without undue delay – notification in phases
  - Risk assessments should not be dependent on forensic reports
  - Preventive and mitigating measures – importance of data breach response plan and training

EDPB Data Breach Guidance

Privacy+ Security Forum

Ransomware Attack	• Importance of adequate backing up • Maximize encryption to prevent data use after exfiltration
Data Exfiltration Attack	• Could attackers modify data in system; recoverability of data; impact on individuals • Identity theft = risk number 1
Internal Human Risk Source	• Risk varies in function of intentional v. unintentional breaches • Importance of employee access policies and controls

EDPB Data Breach Guidance

Privacy+ Security Forum

Lost or Stolen Devices	•Notification expected by default, especially if sensitive data is exposed •Consider investing in remote wiping technology/encryption/device location tracking •Minimize storage of PI on mobile devices, but rather on back-end servers
Misposting	•Common data breach scenario that typically requires notification •Depending on type of data exposed/affected, it may suffice to require recipients who wrongly received data to delete/destroy it •Importance of adequate training, message delays, avoid autocomplete functionalities
Social Engineering	•Attacks through identity theft or impersonation •Invest in robust customer authentication – MFA in function of sensitivity of data •Invest in sound incident detection system

Data Breach Enforcement

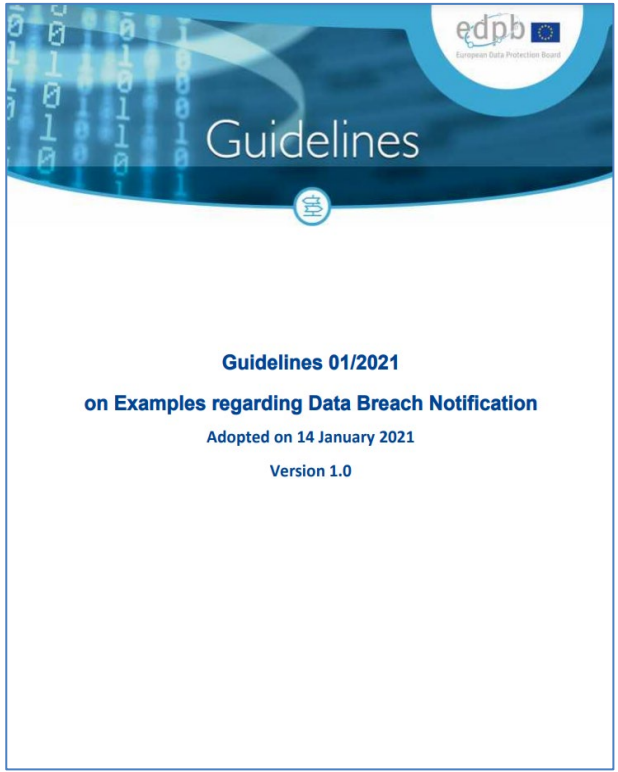
- Notification (or lack of it) often a trigger for Supervisory Authority investigations
- Autoriteit Persoonsgegevens (Dutch SA) fines Booking.com 475K EUR for failure to timely notify
- Spanish DPA decision, 15 March 2021: Fine of EUR 600,000, including specifically amount of EUR 100,000 for a breach of Art. 33 GDPR for notifying the security breach 41 days late.
- Polish DPA decision, 11 January 2021: EUR 30,000 for the controller's failure to report a personal data breach (lack of notification).

Session 4: Practical Exercises

- Data breach cases

Privacy+ Security Forum

EDPB Guidelines 01/2021



Exercise outline

In the context of each of the EDPB case studies

Pre-incident

- What prior measures should be implemented in each case study?
- What factors should be considered as part of the risk assessment?

Post-incident

- What mitigation actions should be taken?
- What obligations apply?

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

Data Exfiltration Attacks

Privacy+ Security Forum

EDPB CASE No. 05: Exfiltration of job application data from a website

An employment agency was the victim of a cyber-attack, which placed a malicious code on its website. This malicious code made personal information submitted through online job application forms and stored on the webserver accessible to unauthorized person(s). 213 such forms are possibly affected, after analysing the affected data it was determined that no special categories of data were affected in the breach.

The particular malware toolkit installed had functionalities that allowed the attacker to remove any history of exfiltration and also allowed processing on the server to be monitored and to have personal data captured. The toolkit was discovered only a month after its installation

Pre-incident

- What prior measures should be implemented in each case study?
- What factors should be considered as part of the risk assessment?

Post-incident

- What mitigation actions should be taken?
- What obligations apply?

Internal Human Risk Source

Privacy+ Security Forum

EDPB CASE No. 08: Exfiltration of business data by a former employee

During his period of notice, the employee of a company copies business data from the company's database he is authorized to access, and needs to fulfil his job.

Months later, after quitting the job, he uses the data thus gained (mainly basic contact data) to contact the clients of the company to entice them to his new business.

Pre-incident

- What prior measures should be implemented in each case study?
- What factors should be considered as part of the risk assessment?

Post-incident

- What mitigation actions should be taken?
- What obligations apply?

Questions

Jan Dhont
Partner, Wilson Sonsini Goodrich & Rosati

Evie Kyriakides
Chief Data Protection & Chief Privacy Officer/ Associate General Counsel, Global Digital, Privacy & Security, Mars, Inc.

John Bowman
Senior Principal, Promontory, an IBM Company