September 29, 2021

EU Privacy+Security Intensive

Jan Dhont
Wilson Sonsini, Brussels

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

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

Privacy+ Security Forum

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
   - The ICO initiative on data transfers
2. **New Issues for 2022 and Beyond**
   - ePrivacy Regulation update
   - AI Regulation update
3. **New EDPB Guidance and one stop shop in practice**
   - EDPB Guidelines on the concepts of controller and processor
   - The one stop shop in practice
4. **Practical Exercises**
   - Controller, processor or joint-controller qualification case

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
- The ICO initiative on data transfers

Privacy+ Security Forum

Background - EU Data Transfer Landscape in Motion

Privacy+ Security Forum

October 6, 2015
The European Court of Justice (ECJ) invalidates the EU-U.S. Safe Harbor (Schrems I ruling)

October 2015 - July 2016
Organizations rush to conclude Standard Contractual Clauses (SCCs) to ensure continuity of transfers previously based on Safe Harbor

July 12, 2016
The EC adopts its adequacy decision for the U.S. (the EU-U.S. Privacy Shield)

July 16, 2020
The ECJ invalidates Privacy Shield (Schrems II ruling)

July 2020 - 2021
Schrems II is put to the test in practice

November 10, 2020
The EDPB adopts its draft Recommendations on supplementary measures

November 12, 2020
The EC publishes draft new SCCs

June 4, 2021
The EC issues final new SCCs

June 18, 2021
The EDPB adopts its final Recommendations on supplementary measures

June 28, 2021
The EC issues its adequacy decision for the UK

2021 - 2022
Expected guidance for ad hoc data transfer agreements and binding corporate rules (BCRs)

What Happened Since Schrems II?

- 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

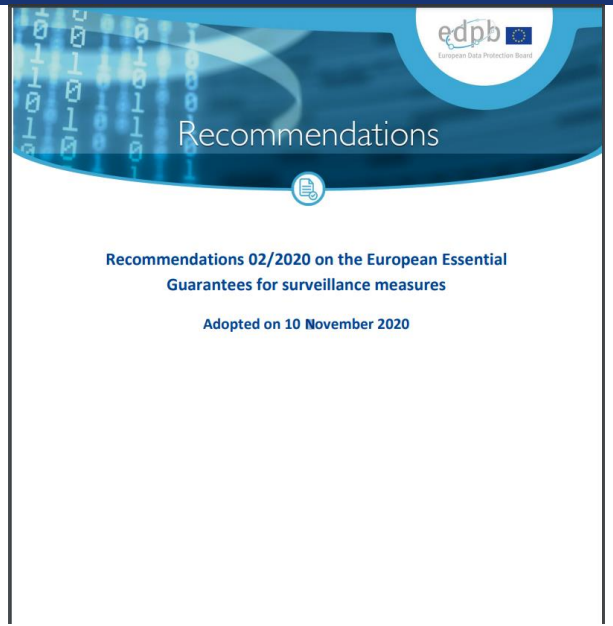
On March 15, 2021, the Bavarian Supervisory Authority (SA)[1] issued a decision regarding the use of Standard Contractual Clauses (SCCs) to transfer personal data from the EU to the U.S. without supplementary security measures. The SA found the data transfer to be unlawful in this case, although it did 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

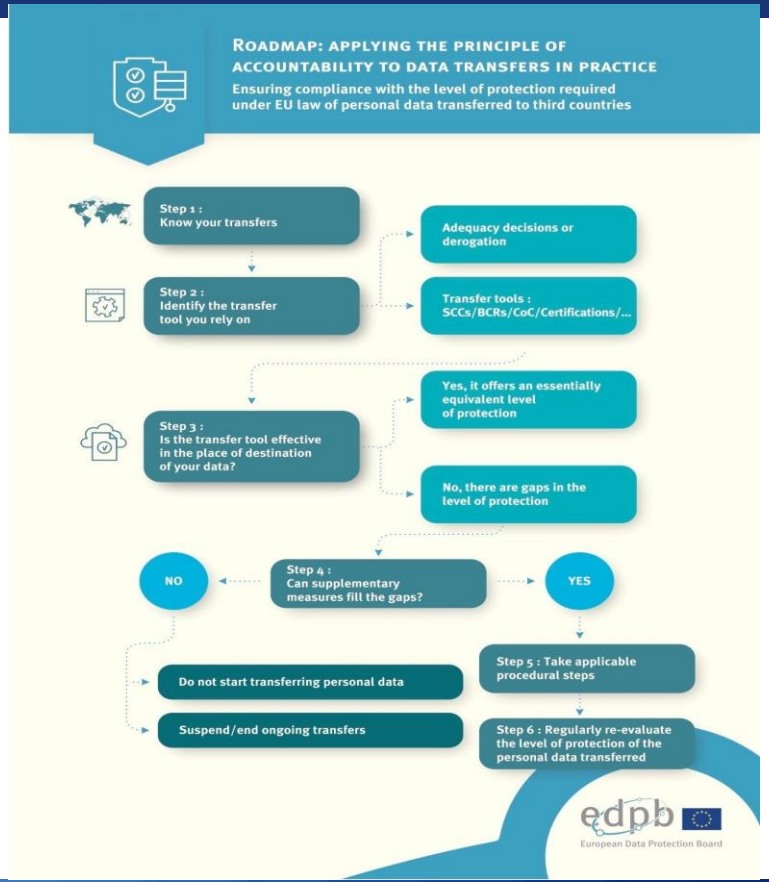
- Roadmap to be followed when transferring personal data outside the EU ("Transfer Tool Recommendations")
- Examples of supplemental measures



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

EDPB Data Transfer Methodology

- 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

Privacy+ Security Forum

Purpose. Determine whether the transfer falls within the scope of legislation and/or practices which may impinge on the effectiveness of the data transfer tool.

Focus. TRA must contain elements concerning access to data by public authorities of the third country of the importer:

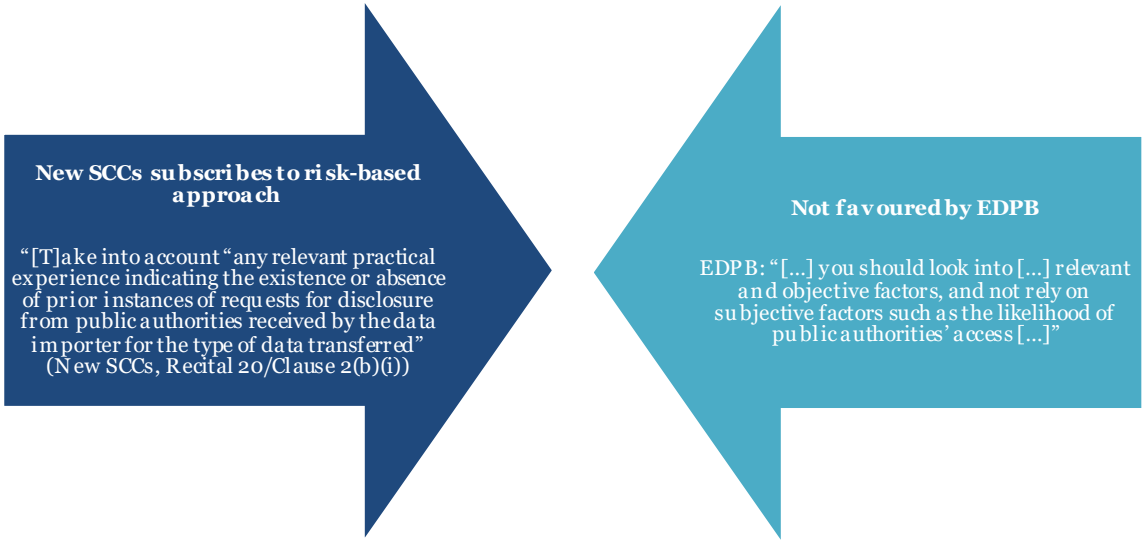
- May public authorities seek potential access in light of legislation, practice and reported precedents?
- May public authorities be able to access through the importer or the telecom provider in light of legislation, practices and reported precedents?
- Tailored to the specific circumstances of the transfer(s)
- Access by public authorities is not intrinsically problematic – question is whether there is due process and available remedies

Step 3 - Transfer Risk Assessment

Findings.

- There is legislation in place that meets the requirements, but is it **effective**?
  - Yes -> no further supplemental measures required
  - No -> supplemental measures
- Appropriate legislation is **lacking**. Are there practices that may undo the protections of the data transfer tool?
  - Yes -> supplemental measures
  - No -> no further supplemental measures required
- The legislation in the third country is "**problematic**".
  - Put supplemental measures in place.
  - Transfer without supplemental measures if "no reason to believe that relevant and problematic legislation will be applied, in practice to the data or the data importer.

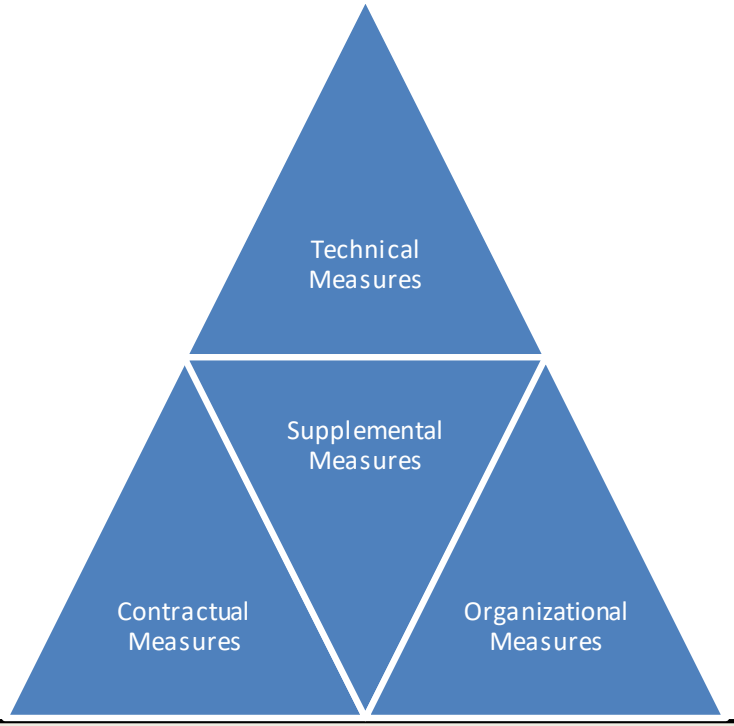
Step 3 - Risk Based Approach (?)



Risk-based approach is now permitted but under conditions. EDPB requires companies demonstrate problematic legislation will "*not be applied in practice*"

SCCs, footnote 12: whether "*practical experience is corroborated and not contradicted by publicly available […] information*"

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

Privacy+ Security Forum

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

Privacy+ Security Forum

- No backdoors that allow access to personal data
- Power for exporter to audit, obtain certifications
- Notify exporter in case of non-compliance/ access by authorities
- “Warrant Canary”
- Obligation for importer to review the legality of access requests and challenge under local law
- Obligation for importer to notify requesting authority about incompatibility of disclosure order with the transfer tool/contractual obligations
- Obligation for importer to assist data subjects to exercise their rights
- Obligation for importer to inform about any onward transfers / commitment not to onward transfer if equivalent protection cannot be ensured
- …

Organizational Measures

- Process to review the legality of any government request and try to challenge or block any disclosure, or provide minimum information possible
- Documentation of data access requests
- 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

- **Practice of conducting TRAs**
  - In practice, often resulting in additional cost and "red-tape"
  - Data exporter questionnaires
  - Data importers conduct assessments to show awareness and preparedness to customers
- **Move towards storing data in the EU where possible**
  - Not always a solution, e.g. if data needs to accessed by the service provider
- **Sectoral differences**
  - Some sectors are more risk averse than others
  - Jurisdictional variation (e.g. Germany)
  - Market position often a factor of level or risk averseness

Session 1: Data Transfers Post-Schrems II

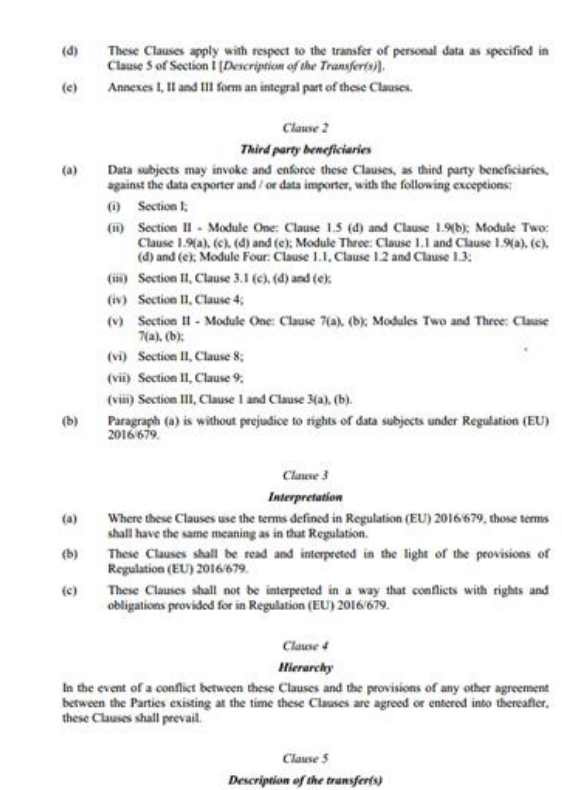
- The New Standard Contractual Clauses

Privacy+ Security Forum

Why New SCCs?

- **Alignment with GDPR**
  - Higher threshold of data protection than Framework Directive 95/46
- **Flexibility for businesses**
  - Old SCCs did not accommodate processor data exports
- **Schrems II**
  - SCCs are the most popular data transfer tool
  - Schrems II clauses

What Do The New SCCs Look Like?



(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**: Local laws and obligations in case of access by public authorities
  - **Section 4:** Final provisions on 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 Novelties

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)

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 TRA / 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

Implementing The New SCCs

1. Timeframe

- "Old SCCs" could be executed until September 27, 2021
- "Old SCCs" currently executed can be relied on until December 27, 2022, unless modifications are made (e.g., new categories of data added, new parties added etc.)

2. Strategizing

- Data importers should consider reviewing DPAs and foreseeing a process for contract upgrade (existing customers v. new customers)
- Data exporters should equally strategize on reviewing SCCs in place with importers
- Intra-group agreement refresher
- Simple use of SCCs or keep using DPAs and attach SCCs?
- What about data exports from the UK?

3. How to implement the SCCs in practice?

- Start from the framework provisions
- Select the relevant module
- Sign as a standalone contract or include into existing contracts
- Practice of incorporation via referencing
- "Hybrid" data processing (processor with limited re-use for own purposes -> combination of C2C and C2P)

Ensure Effective Compliance

Privacy+ Security Forum

Data Exporters

1. Take stock of data transfers and conduct TRAs
   - Use of Article 30 records
   - Use of data transfer due diligence questionnaires
   - Potential prioritization ("high" v. "low risk" exports)
2. Implement any additional supplemental measures in light of TRA outcome
3. Ensure effective compliance with SCC obligations
   - Obligations vary depending on module (more exporter obligations in P2P and P2C modules)
   - Transparency and data subject right requirements (assistance of data importer where needed)
   - Process to deal with data breach issues under the SCCs – streamline action with the importer where required
   - Ensure strict diligence of onward transfers
   - Be able to demonstrate compliance with the SCCs (accountability)
4. Joint and several liability regime

Data Importers

1. Take stock of onward transfers and conduct TRAs
   - Provide comfort to exporters by assessing possible need for supplemental measures
   - Understand obligations to disclose data to local public authorities (clause 14 SCCs)
2. Update relevant agreements
   - DPAs/MSAs with exporters
   - DPAs/Onward transfer agreements with sub-processors
3. Ensure effective compliance with SCC obligations
   - Process to monitor appropriateness of information security and to deal with data breach notification requirements
   - Process to deal with data subject rights
   - Process to deal with "Schrems II" obligations (clauses 14 and 15 SCCs)
   - Keep appropriate documentation of compliance / accountability
   - Acceptance of jurisdiction competent SA / cooperation obligations
4. Anticipate potential liability
   - Hold sub-processors liable for non-compliance
   - Governing law and forum will mostly not follow law of MSA (clauses 17 and 18 SCCs)

Open Issues

1. Relationship between the New SCCs and Article 3(2) GDPR

- Need for non-EU organizations directly subject to the GDPR to conclude SCCs (Art. 3(2) GDPR)?

2. Assessing the level of protection in the country of import – "risk-based" approach

- Welcome flexibility: practical experience is relevant under strict conditions
- Courts are likely to pave the way

3. What constitutes 'appropriate supplementary measures' remains unclear in certain situations

- U.S. companies subject to FISA, data transfers to Russia or China
- Focus on technical safeguards such as encryption, but its applicability remains limited in practice
- EDPB suggests burdensome audit rights to allow data exporters to verify disclosures to public authorities

Open Issues

4. Certain obligations do not respect the business relationship

- Sub-processor must contact the controller in certain circumstances

5. Long arm

- Very restrictive onward transfer regime

6. Enforcement against data (the) importer(s) by EU SAs (?)

7. Data transfers from, and to, the UK

- New SCCs do not enable transfers from the UK

Recent Post-Schrems II Developments

Privacy+ Security Forum

Cases on transfers to the U.S.

- In August 2021, the Hamburg SA officially warned the regional Senate Chancellery to stop using Zoom because of insufficient protection of data transmitted to the U.S.
- In August 2021, the Belgian's Council of State concluded that the applicants failed to prove that transfers to the U.S. were in violation of the GDPR.
- In May 2021, the EDPS opened two investigations regarding AWS and Microsoft cloud services, and the use of Microsoft Office 365.
- In April 2021, the Portuguese SA (CNPD) ordered the National Institute for Statistics to suspend sending personal data to the U.S. The INE outsourced the operation of the census questionnaire to American company Cloudflare, Inc.

Transfers to China & other third countries

- In September 2021, the Irish SA announced that it launched investigation into TikTok's data transfers to China.
- In July 2021, the Hessen SA ordered a German laboratory operator to cease data transfers to China.
- In June 2021, the German SAs announced a coordinated nationwide investigation concerning international transfers. Participating SAs contact companies individually with a standardized questionnaire and then analyze the answers and decide on further steps.

UK ICO and International Data Transfers

Privacy+ Security Forum

> ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK

Consultation Start Date **11 August 2021**
Type **ICO consultation, Open**

> This consultation closes on 07 October 2021;

The consultation is split into three sections, offering a selection of proposals and options to consider.

1. Proposal and plans for updates to guidance on international transfers.
2. Transfer risk assessments.
3. The international data transfer agreement.

Transfer Risk Assessment and Tool

Privacy+ Security Forum

Three step approach for routine restrricted transfers

The transfer risk tool

Step one: Assessing the transfer

Decision tree	
Does the transfer comply with the rest of the UK GDPR?	
Yes ↓	No **TRA tool not suitable**
Is this TRA tool suitable for your transfer risk assessment?	
Yes ↓	No **TRA tool not suitable**
Record the specific circumstances of the transfer	
↓ **Go to Step 2**	

Step two: Is the IDTA likely to be enforceable in the destination country?

In the first part of this step, you will assess the enforceability of the contractual safeguards that the IDTA provides in the destination country. If this satisfies you, you can move on to step three. If you have concerns,

you should carry out the extra steps and protections assessment that the second part of step two outlines.

Decision tree			
Step 2A Are the contractual safeguards likely to be enforceable in the destination country?			
Yes ↓	Don't know ↓ Assume serious concerns	No ↓	
Go to Step 3	Step 2B Taking into account the specific circumstances of the transfer and your concerns about the destination country regime, what is the risk of harm to individuals		
	Low risk ↓	Enhanced risk ↓	
	Go to Step 3	Are you able to take extra steps and protections to reduce the risk of harm to low risk?	
		Yes ↓ **Go to Step 3**	No ↓ **TRA tool not suitable**

Step three: Is there appropriate protection for the data from third-party access?

In step three you assess the destination country's regime for regulating third-party data access, including surveillance.

Decision tree				
Is the destination country's regime similar enough to the UK's regime in terms of regulating third party access to data (including surveillance)?				
Yes ↓	Don't know ↓ Assume serious concerns	No ↓		
Make the transfer	How likely is third party access to the data (including surveillance)?			
	Minimal risk ↓ **Make the transfer**	Don't know ↓ Assume more than a minimal risk ↓	More than a minimal risk ↓	
		Considering the circumstances of the transfer and the destination country's regime, what is the risk of harm to data subjects?		
		Low risk ↓ **Make the transfer**	Enhanced risk ↓ Are you able to take extra steps and protections to reduce the risk of harm to low risk?	
			Yes ↓ **Make the transfer**	No ↓ **TRA tool not suitable**

International Data Transfer Agreement

Privacy+ Security Forum

Draft International data transfer agreement

August 2021

ico.
Information Commissioner's Office

Part one: Tables

[Instructions: We provide a template format, but you do not need to use it. Just make sure that you provide all the information set out in the table below and that the Mandatory Clauses correctly cross-refer to this information.]

Table 1: Parties and signatures

Start Date	[Instructions: Insert start date of IDTA. If the parties agree, the start date can be either before or after both have signed.]	
The Parties	**Exporter (who sends the restricted transfer)**	**Importer (who receives the restricted transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):

Part two: Extra Protection Clauses

[Instructions: We provide a template format, but you do not need to use it. Just make sure that you provide all of the information set out in the table below and that the Mandatory Clauses correctly cross-refer to this information.]

Extra Protection Clauses:	[Instructions: If, having considered the protections available to the Transferred Data and any TRA, you decide that you need extra steps and protections in order to maintain the right level of protection in the IDTA, those extra steps and protections must be set out in clauses in this IDTA. You may add those clauses in here.]
(i) Extra technical security protections	[Instructions: these are additional technical security protections. You may choose to include these in Table 4 Security Requirements. If so, you do not need to set them out here. However, it can be helpful to include them here (or cross refer to them) for when you review the IDTA.]
(ii) Extra organisational protections	[Instructions: these are additional organisational protections. For additional organisational security protections, you may choose to include them in Table 4 Security Requirements. If so, you do not need to set them out here. However, it can be helpful to include them here (or cross refer to them) for when you review the IDTA.]

International Data Transfer Agreement/2

Part three: Commercial Clauses

[Instructions: You may add commercial clauses, but you are not required to do so.

We provide a template format, but you do not need to use it. For example, you may not need to add any Commercial Clauses if you have a Linked Agreement.

If you are not using any Commercial Clauses, the simplest thing to do is to state "Commercial Clauses are not used" in this section.

You must be cautious when adding in commercial clauses. If you inadvertently reduce the level of protection in the IDTA then those commercial clauses will not be enforceable and your restricted transfer may be in breach of UK GDPR.]

Commercial Clauses	[Instructions: Insert additional commercial clauses agreed by the Parties, if any.]

Part four: Mandatory Clauses[8]

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

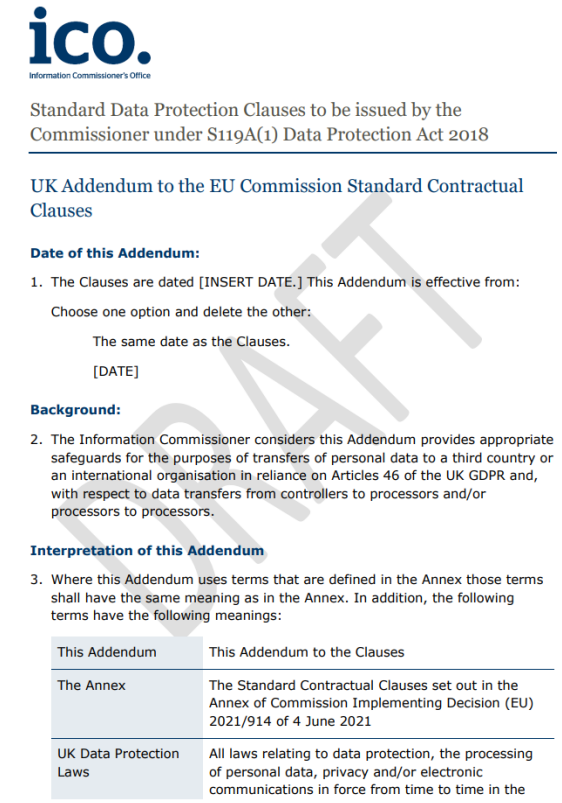
1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Data and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Parties confirm that there is a Linked Agreement between the Parties which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with this IDTA.

UK Addendum to EU SCCs



ico.
Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

Date of this Addendum:

1. The Clauses are dated [INSERT DATE.] This Addendum is effective from:

   Choose one option and delete the other:

   The same date as the Clauses.

   [DATE]

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the

Amends EU SCCs to work in UK context

The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

a) for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

b) to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

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

Privacy+ Security Forum

- 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

- **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

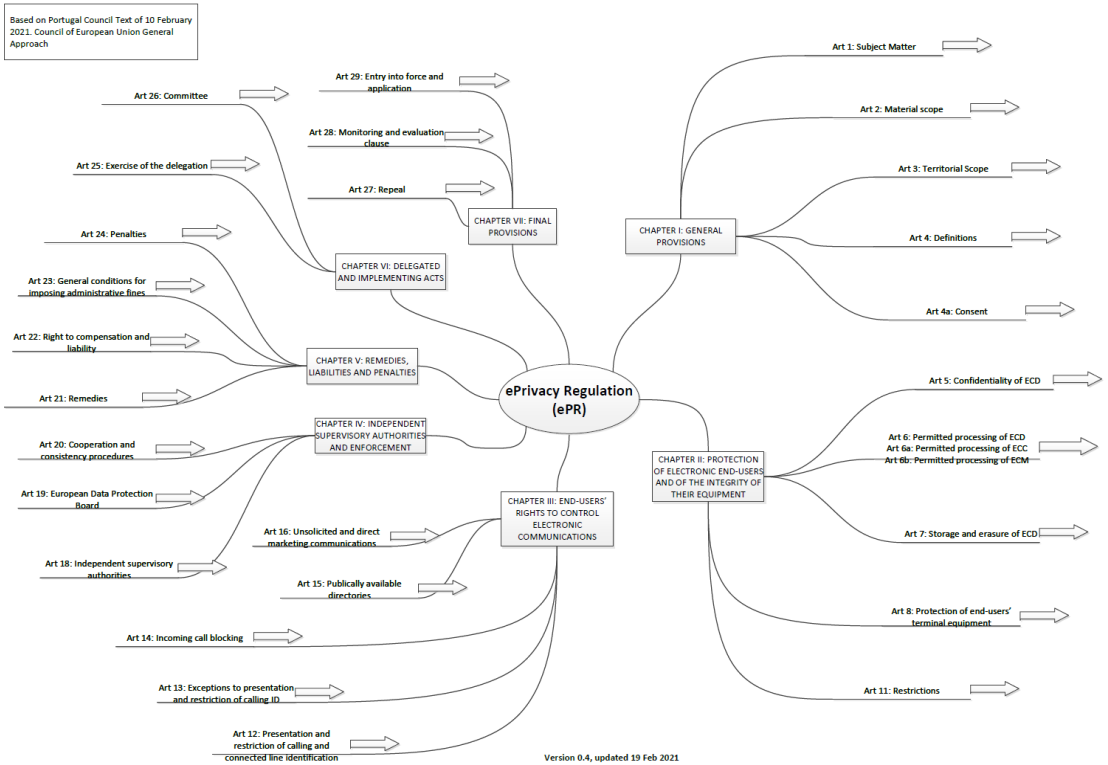
- **Last resort derogation**
  - Data exporter must be able to demonstrate that it was not possible to rely on Article 45 and 46 GDPR or any of the other Article 49 GDPR derogations
- **Compelling legitimate interests of the controller**
  - E.g. "*if a data controller is compelled to transfer personal 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 2022 and Beyond

- ePrivacy Regulation update
- AI Regulation update

Privacy+ Security Forum

ePrivacy Regulation update

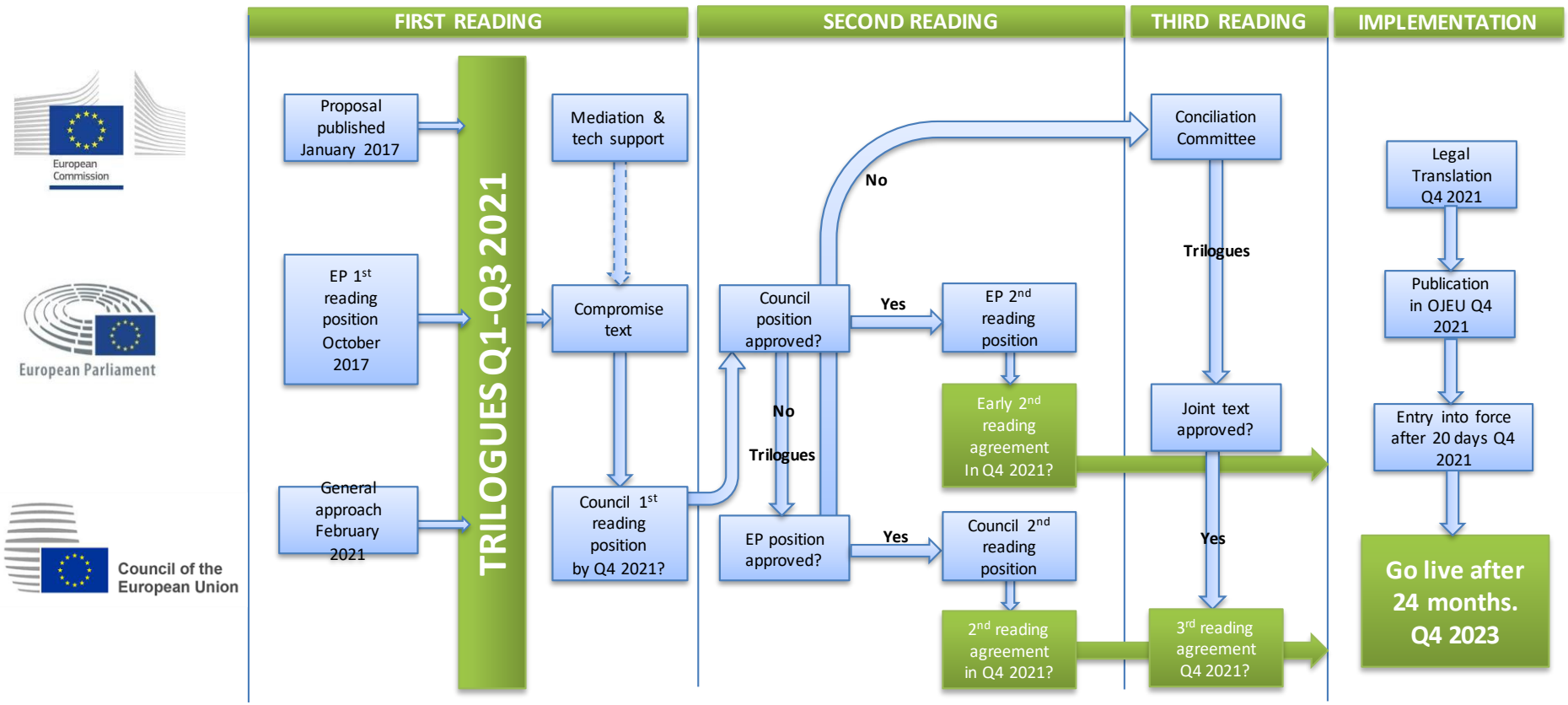


Main features of ePR

- 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)

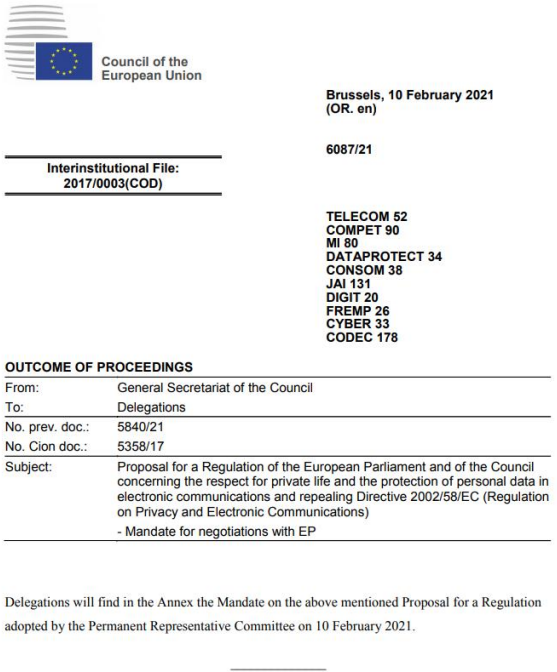
Path to agreement

Privacy+ Security Forum



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.

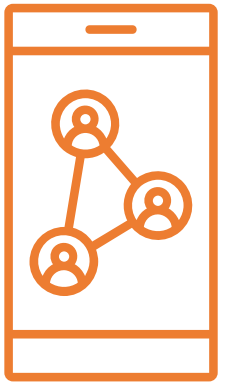
Electronic communications are the keystone of many essential activities of our modern societies, since they support the exercise of many fundamental rights such as freedom of thought, conscience, religion, expression, information, assembly, association, etc. Reinforcing the confidentiality and neutrality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



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

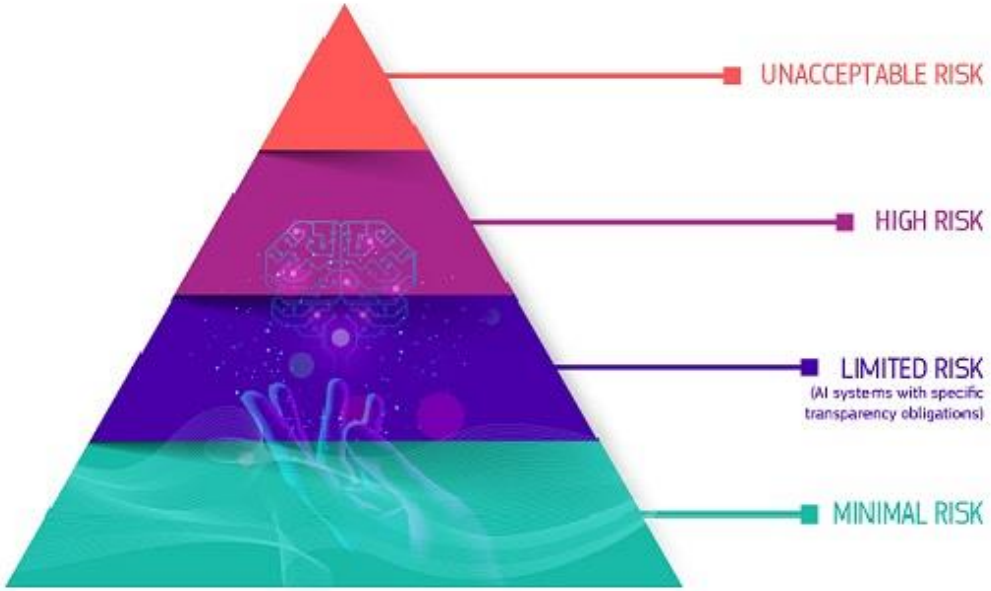
- All providers who offers AI services in the EEA
- All users of AI in the EEA
- Where AI outputs are utilised in the EEA

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

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.

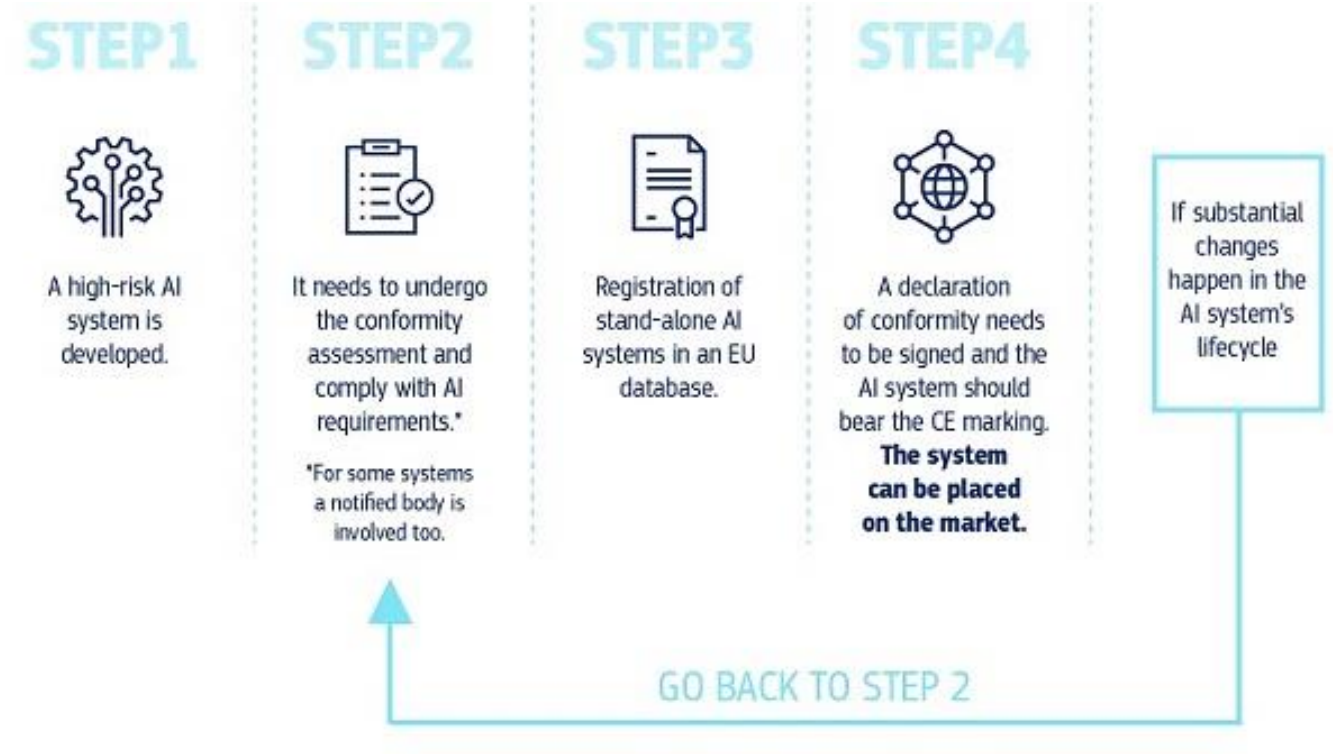
• **Unacceptable Risk;** systems which pose a clear threat to the safety, livelihoods and rights of individuals will be banned (e.g. social scoring by governments).

• **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 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

- The EDPB Guidelines on the concepts of controller and processor in the GDPR
- The one-stop shop in practice

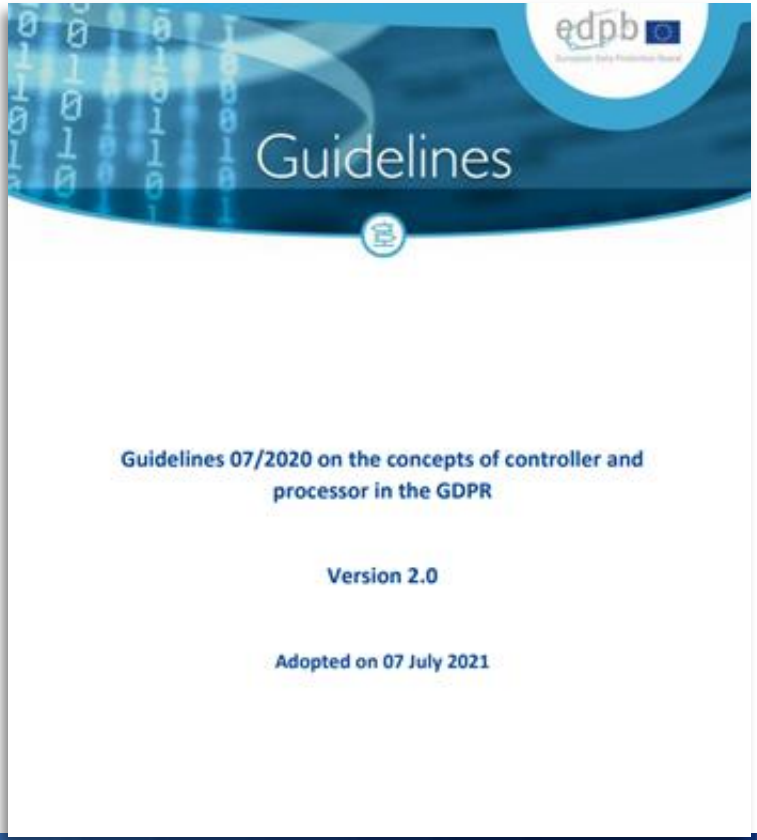
Privacy+ Security Forum

EDPB Guidelines on the Concepts of Controller and Processor

Privacy+ Security Forum

Detailed insights on concepts of:

- controller
- joint controller
- processor
- sub-processor
- third party/recipient
- contract/other legal act between controller and processor
- arrangement between joint controllers



EDPB Guidelines on the Concepts of Controller and Processor

Privacy+ Security Forum

Controller

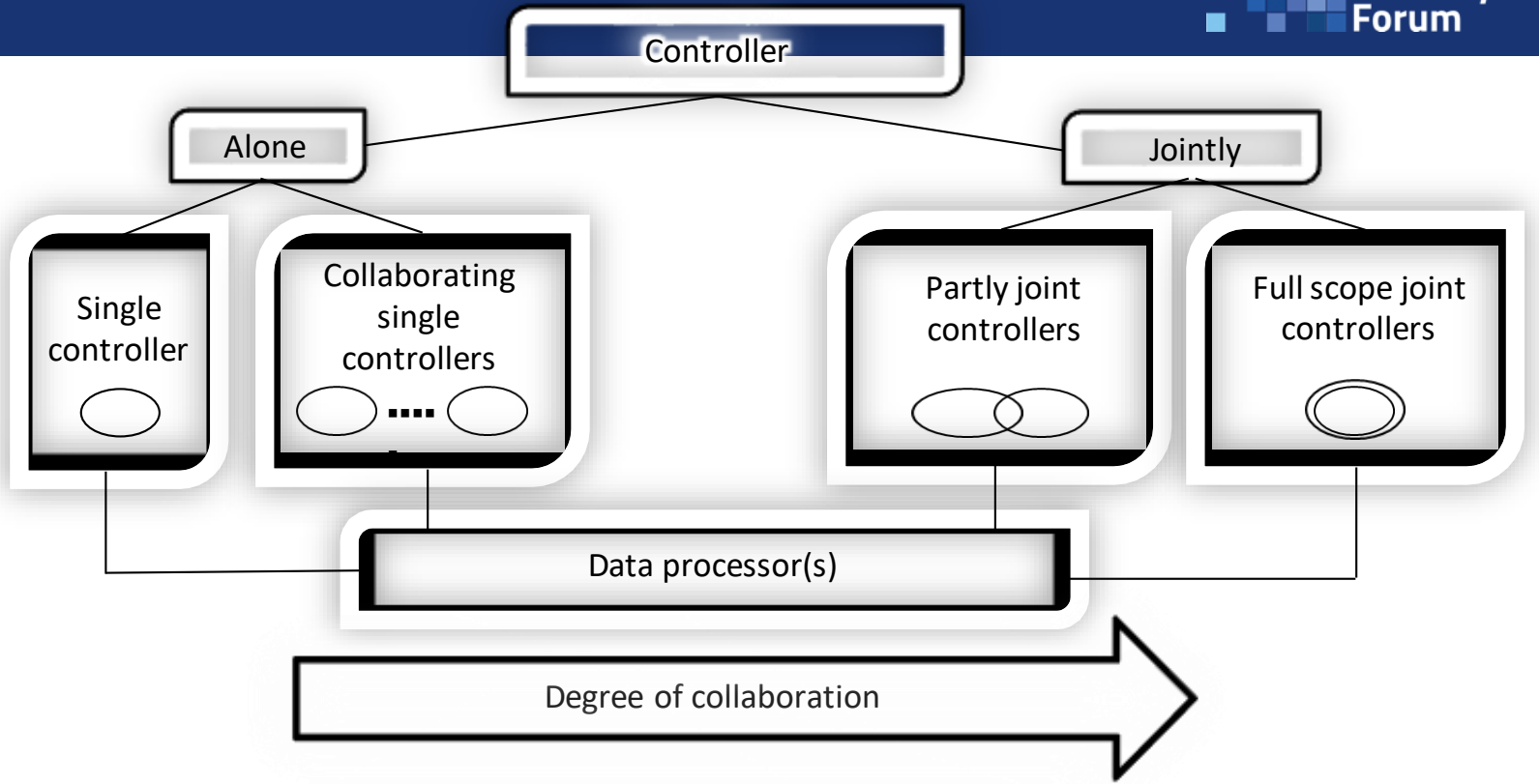
- determines both purposes and essential means of processing
- give instructions on purposes and means of processing
- does not need to have access to processed data
- must make the final decision to actively approve the way the processing is carried out and request changes if necessary
- must only use processors providing sufficient guarantees to implement appropriate technical and organizational measures
- needs to be bound by a contract/other legal act with processor

≠

Processor

- never determines purposes and essential means of processing, but can decide on some non-essential means, i.e., more practical aspects of implementation
- receives and follows instructions on purposes and means of processing - processes personal data on behalf of controller
- is a separate entity in relation to the controller
- needs to be bound by a contract/other legal act with controller and, if applicable, sub-processor

VARIABLE SCALE OF CONTROL



Source: T. Olsen and T. Mahler (on the basis of WP29)

Joint Controllers - EDPB Guidelines on the Concepts of Controller and Processor

- the fact that one of the parties does **not have access** to processed personal data, or
- the fact that parties involved in the processing of personal data share **unequal responsibilities**, or
- the fact that the entities do **not pursue the same purposes** but purposes which are **closely linked / complementary**

does not exclude joint controllership

- the fact that the processing involves **several entities**, or
- The mere existence of a **mutual benefit** (e.g., commercial) arising from a processing activity

does not necessarily give rise to joint controllership

JOINT CONTROLLERS' ARRANGEMENT

Privacy+ Security Forum

Who will provide information to the data subjects?

Who will report data breaches?

Who will reply to data subjects' requests?

Cooperation to conduct DPIAs

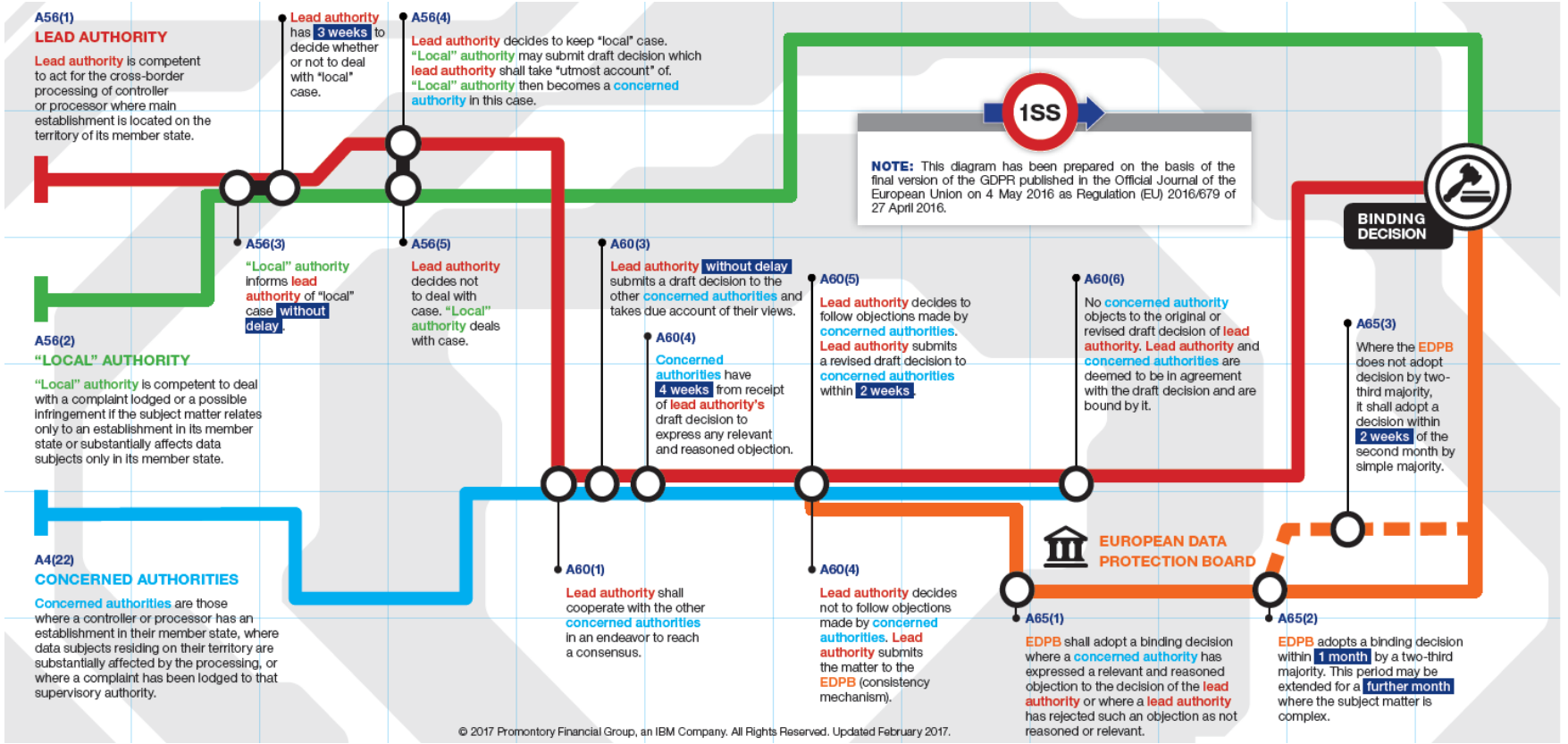
Will processors be engaged?

SOME PRACTICAL CONSIDERATIONS

Privacy+ Security Forum

- Joint controller v. separate controller?
- Same group companies v. external
- Update Article 30 records
- Joint-Control Arrangements
  - Delineate the joint control operations
  - Clearly allocate responsibilities/associated liabilities
- Data Processing Arrangements
  - In grey zone situations, indicate intent (not) to establish joint-control (if necessary with “fall-back” arrangement)
- Consider best protection of the data subject

One-stop shop in practice



Key decisions

15 December 2020 Ireland

The Data Protection Commission (DPC) has today announced a conclusion to a GDPR investigation it conducted into **Twitter International Company**. The DPC's investigation commenced in January, 2019 following receipt of a breach notification from Twitter and the DPC has found that Twitter infringed Article 33(1) and 33(5) of the GDPR in terms of a failure to notify the breach on time to the DPC and a failure to adequately document the breach. The DPC has imposed Tan **administrative fine of €450,000** on Twitter as an effective, proportionate and dissuasive measure.

2 September 2021 EDPB

On July 28th, the EDPB adopted a dispute resolution decision on the basis of Art. 65 GDPR. This binding decision seeks to address the dispute arisen following a draft decision issued by the Irish (IE) SA as lead supervisory authority (LSA) regarding **WhatsApp Ireland Ltd.** (WhatsApp IE) and the subsequent objections expressed by a number of concerned supervisory authorities (CSAs). In accordance with the GDPR, the EDPB's binding decision has now been published, following the notification of the IE SA's final decision to the company.

In this case, the EDPB found the consolidated turnover of the parent company (Facebook Inc.) is to be included in the turnover calculation.

Session 4: Practical Exercises

- Controller, processor or joint-controller qualification case

Privacy+ Security Forum

Case 1

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions.

Can companies A and B be considered joint controllers? Why (not)?

Case 2

The Brussels-based HQs of a multinational decide to use a HRM software provider located in the EU for all their HR operations. Various providers were reviewed during the procurement process and the multinational also involved the group entities to ensure that the provider satisfies their operational needs. Ultimately vendor Y was chosen and a service agreement was put in place between the HQ of the multinational and the vendor for provision of services.

How do you qualify the parties with respect to the HRM application?

1. Service provider
2. The HQ of the multinational
3. The group entities of the multinational

Questions

Jan Dhont
Partner, Wilson Sonsini Goodrich & Rosati

John Bowman
Senior Principal, Promontory, an IBM Company