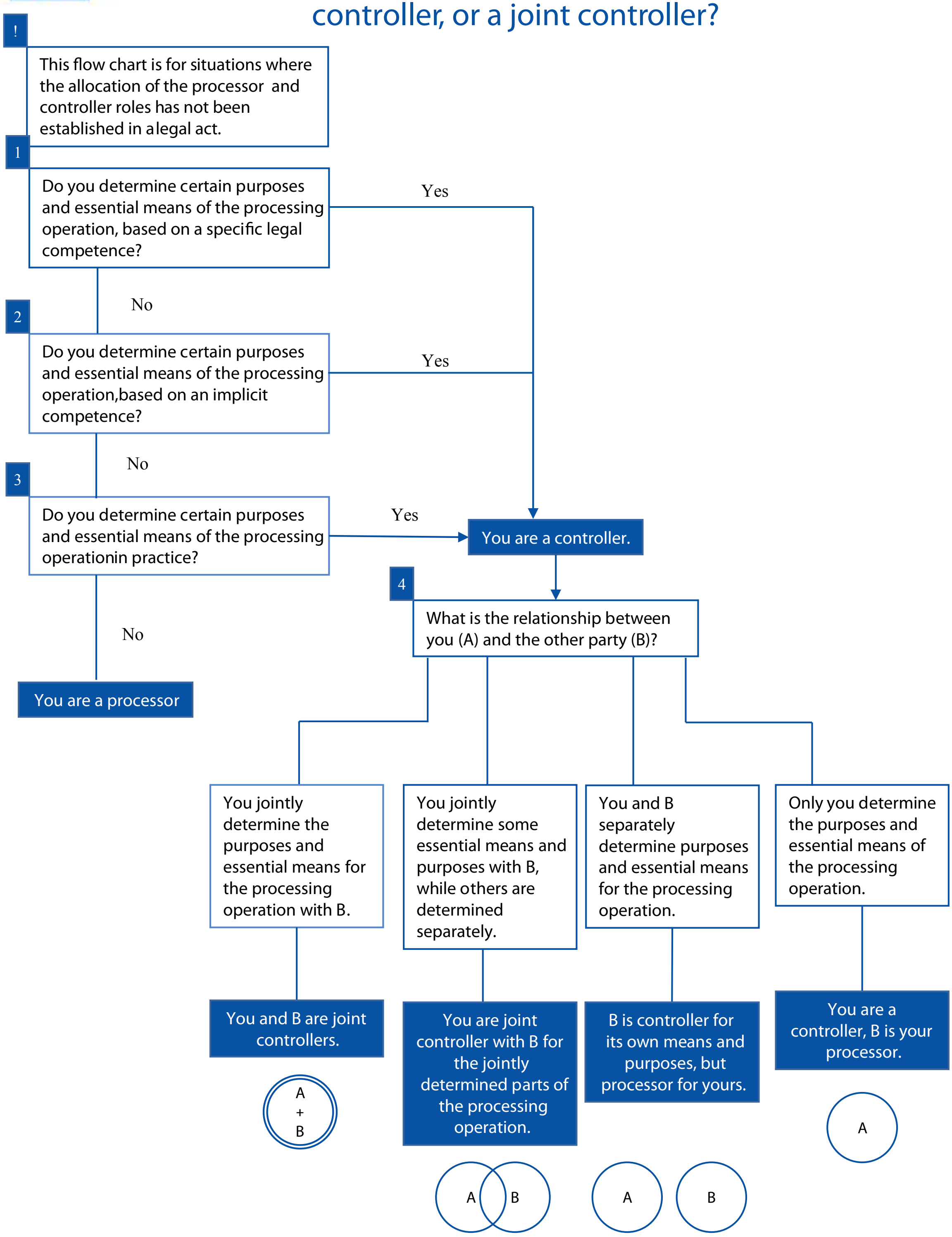
EDPS

Flowcharts and Checklists on Data Protection

PDF ISBN 978-92-9242-461-9 doi: 10.2804/823679 QT-02-20-505-EN-C
PRINT ISBN 978-92-9242-462-6 doi: 10.2804/912368 QT-02-20-505-EN-N

Are you a processor, controller or joint controller?

Flowchart for EUIs. You are involved in a processing operation with one or more third parties: are you a processor, a controller, or a joint controller?



!
This flow chart is for situations where the allocation of the processor and controller roles has not been established in alegal act.
1
Do you determine certain purposes and essential means of the processing operation, based on a specific legal competence?
Yes
No
2
Do you determine certain purposes and essential means of the processing operation,based on an implicit competence?
Yes
No
3
Do you determine certain purposes and essential means of the processing operationin practice?
Yes
No
You are a processor
You are a controller.
4
What is the relationship between you (A) and the other party (B)?
You jointly determine the purposes and essential means for the processing operation with B.
You jointly determine some essential means and purposes with B, while others are determined separately.
You and B separately determine purposes and essential means for the processing operation.
Only you determine the purposes and essential means of the processing operation.
You and B are joint controllers.
You are joint controller with B for the jointly determined parts of the processing operation.
B is controller for its own means and purposes, but processor for yours.
You are a controller, B is your processor.
A + B
A
B
A
B
A

Note: The aim of this flowchart is to clarify the initial qualification as controller or processor, rather than setting out what happens when a processor exceeds its mandate/role by becoming involved in determining essential means of the processing.

Checklist 1: What are the duties of the controller?

Processing of personal data needs to adhere to the following **principles**:

- the processing operation should be lawful, fair and transparent (**lawfulness, fairness, transparency**);
- the processing operation should be bound to specific purposes (**purpose limitation**);
- the personal data processed should be adequate, relevant and limited to what is necessary (**data minimisation**);
- the personal data should be accurate (**accuracy**);
- the personal data should be kept no longer than necessary (**storage limitation**);
- the personal data need to be remain well secured and confidential (**integrity and confidentiality**).

See the EDPS guide Accountability on the ground, part II, pages 11-15 for guiding questions on these data protection principles.

The controller is responsible for compliance with these principles and should be able to demonstrate this compliance (principle of accountability). To achieve this, controllers in practice need to, in particular:

- document their processing operations with **records**; (Note: the EDPS strongly recommends keeping these records in a **central, publicly accessible register**);
- carry out a data protection impact assessment (**DPIA**), prior to operations which carry a high risk to the rights and freedoms of data subjects;
- under certain circumstances, **consult the EDPS** prior to such high-risk processing operations;
- when designing processing operations, keep in mind the principles of **privacy by design** and **privacy by default**;
- take **adequate security measures** in order to protect personal data;
- in case of a **personal data breach**, notify the EDPS as well as, under certain circumstances, the data subjects involved;
- conclude **agreements/contracts with processors** (only those providing sufficient guarantees);
- conclude agreements with other controllers in cases of **joint controllership**;
- **transfer** personal data within the European Institution, agency or body (EUI), to other EUIs, to countries outside of the EU or international organisations only when the conditions of the Regulation (EU) 2018/1725 are complied with;
- **cooperate with the EDPS**.

See the EDPS **Accountability on the ground** for guidance on records, DPIA's, prior consultation and more.

Finally, the controller need to provide clear and accessible information to data subjects about the processing, respect data subject's rights and ensure their availability in practice.

See the EDPS guidelines on transparency and other rights and obligation.

Know your processing operations

Article 4 of EUDPR lists the **data protection principles**. Additional Articles in this Regulation spell them out in more detail:

DP principle	Articles	Recitals
Fairness	Article 4(1), 17 to 25	20, 26, 34, 35, 37-41
Transparency	Articles 4(1)(a), 14 to 16, 25	20, 35, 36
Purpose limitation	Articles 4(1)(b), 6, 13, 38	25
Data minimisation	Articles 4(1)(c), 12, 13, 37, 38	20
Accuracy	Articles 4(1)(d), 18	38
Storage limitation	Articles 4(1)(e), 13	20, 33
Security	Articles 4(1)(f), 33, 36, 37, 39	53, 54, 58

Create a systematic description of the processing. Start from the information you already have in your notification or record and add the following points:

- **data flow diagram** of the process (flowchart): what do we collect from where/whom, what do we do with it, where do we keep it, to whom do we give it?
- **detailed description of the purpose(s)** of the processing: explain the process step-by-step, distinguishing between purposes where necessary;
- **description of its interactions with other processes** - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?
- **description of the supporting infrastructure**: filing systems, ICT etc.

Use existing documentation of the process or its development to generate this documentation. Re-read this existing documentation through the lens of "how will this affect the people whose data we process?" and adapt and expand where necessary.

Go through your data flow diagram and for each step, ask yourself how this could affect the persons concerned against the background of the data protection principles.

The table below maps the targets to some generic processing steps, indicating the most relevant targets for each. These are the **minimum aspects to check**.

Lawfulness is to be ensured as the first stage and at each processing step.

	Fairness	Transparency	Purpose Limitation	Data minimisation	Storage limitation	Security
Collection	X	X	X	X		X
Merging datasets	X	X	X	X		X
Organisation/structures			X	X		
Retrieval/consultation/ use	X	X	X		X	X
Editing/alteration		X		X		X
Disclosure/Transfer	X	X	X	X		X
Restriction			X	X	X	X
Storage	X	X	X		X	X
Erasure/destruction			X		X	X

See the EDPS **Accountability on the ground** guidance, part II, pages 7, 9-11 for mapping data protection principles to generic processing steps.

Checklist 2:
What are the duties of the processor?

In order to comply with Regulation (EU) 2018/1725 (EUDPR), processors must in particular:

- only process personal data on the **documented instructions of the controller**, unless required to do so by EU or Member State law;
- process personal data as **governed by a contract or legal act** which is binding on the processor and that sets out the necessary prerequisites for the processing activity;
- **NOT further process** data for other incompatible purposes;
- **assist the controller** with the obligation to guarantee the **rights of data subjects** and to fulfil the controllers **obligations pursuant to Articles 33-41** EUDPR (security and data breach notification, data protection impact assessment and prior consultation, confidentiality of electronic communications, information and consultation of EDPS);
- **notify** any legally **binding request for disclosure** of the personal data processed on behalf of the controller and may only give access to data with the prior written authorisation of the controller;
- **ONLY outsource/subcontract with the prior written authorisation** of the controller; inform controller of any changes, giving controller the opportunity to object; pass on same contractual obligations to any subcontractors;
- **maintain a record** of all categories of processing activities carried out on behalf of the controller;
- take **adequate security measures** in order to protect the personal data;
- without undue delay, inform the controller of a **data breach**;
- **cooperate**, on request, with the EDPS in the performance of his or her tasks.

Checklist 3: What is required in a processing agreement?

Controllers can have another entity process personal data on their behalf. Outsourced processing thus concerns personal data produced and processed by the contract, not data of the contractor or its staff.

Processing by a processor requires a **contract or other legal act** under EU or Member State law, which is **binding on the processor** and sets out:

- purpose, duration, nature and scope of processing;
- categories of data and data subjects;
- retention period;
- data location and data access (based on preliminary risk assessment may be limited or not to EEA);
- recipients of data and data transfers (within the EUI, to other EUIs, to third countries or international organisations);
- security measures (guaranteeing at minimum the same level of security for the personal data as the controller);
- prohibition of disclosure of data – reference to the Protocol on Privileges and Immunities of the EU;
- any additional data protection laws (e.g. ePrivacy Directive, NIS Directive) – if applicable;
- processor may only act upon documented instructions of controller, unless required to do so by EU or Member State law (instructions also on transfers of personal data and assistance to controller);
- sub-contracting only with prior written authorisation of controller, information in due time before any changes;
- confidentiality measures, access only on a need to know basis to authorised persons;
- auditing rights by controller of processors and sub-processors;

- cooperation, on request, with the EDPS in the performance of his or her tasks (including EDPS' audit / investigation of processors and sub-processors);

- division of tasks between joint controllers – if applicable – so that processor knows how to assist which joint controller;

- assistance with data subject rights requests;

- assistance with controller obligations (security and data breach notification, data protection impact assessment and prior consultation, confidentiality of electronic communications, information and consultation of EDPS) and record of processing on behalf of controller;

- assistance with data breaches – set specific deadline;

- choice by controller for processor to return or delete the data at the end of the processing;

- obligation to inform the controller if its instruction infringes Regulation (EU) 2018/1725 or other EU or Member State data protection provisions;

- ground for termination in case of substantial non-compliance of processor, liability etc.;

- applicable data protection law;

- other applicable provisions affecting data protection, e.g. choice of applicable law and jurisdiction (Member State of EUI's seat), amendments (only bilateral) etc.

The contract or other legal act may be based, in whole or in part, on **standard contractual clauses for processors adopted by the EDPS or the EC**.

Useful hints and questions on data protection

Main lines

- Think about what you need to do to fulfil your business needs and limit yourselves to it.
- Define what you do, document it.
- Tell people about it and respect their rights.

Some useful questions

- What exactly do we want to do and why?
- Why are we allowed to do it?
- What data do we need to do it and for how long?
- Who needs to have access to the data?
- How do we make sure it is not used otherwise?
- How do we tell people about it and give them access to their data?
- How do we document all this?
- Want to know more? Need guidance? Talk to your Data Protection Officer. Document every step for accountability purposes.

Why informing people about data processing?

So that they can:

- understand which of their data are processed and how;
- verify the quality of their own data;
- exercise their other data protection rights (access, rectification, erasure, restriction of processing, notification of rectification, erasure, restriction of processing, data portability, objection, not to be subject to a decision based solely on automated processing, including profiling).

Guiding questions on fairness

- Can people expect this to happen, also if they do not read the information you provide them with?
- In case you rely on consent, is it really free? How do you document that people gave it? How can they revoke their consent?
- Could this generate chilling effects?
- Could this lead to discrimination?
- Is it easy for people to exercise their rights to access, rectification, etc.?

Data protection factors when publishing personal data

- Am I obliged to publish? May I publish? (Legal basis)
- What can I publish? (Data minimisation)
- How do I tell the individuals concerned? (Information)
- How do I make sure the data is correct? (Accuracy)

Guiding questions on transparency

- How will you tell people about your processing?
- How do you make sure the information reaches the persons affected?
- Have you provided all the information necessary and is it easy to understand?
- Is the language tailored for the audience For example, children?
- In the event that you defer providing information, what is your justification?

Guiding questions on purpose limitation

- Have you identified all the purposes of your process?
- Are all purposes compatible with the initial purpose?
- Is there a risk that the data could be reused for other purposes (function creep)?
- How can you ensure that data are only used for their defined purposes?
- If you want to make available/re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

Guiding questions on data minimisation

- Are the data of sufficient quality for the purpose?
- Do the data you collect measure what you intend to measure?
- Are there data items you could remove without compromising the purpose of the process?
- Do you clearly distinguish between mandatory and optional items in forms?
- In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

Guiding questions on storage limitation

- Does EU legislation define storage periods for your process?
- How long do you need to keep which data? For which purpose(s)?
- Can you distinguish storage periods for different parts of the data?
- If you cannot delete the data just yet, can you restrict access to it?
- Will your tools allow automated erasure at the end of the storage period?

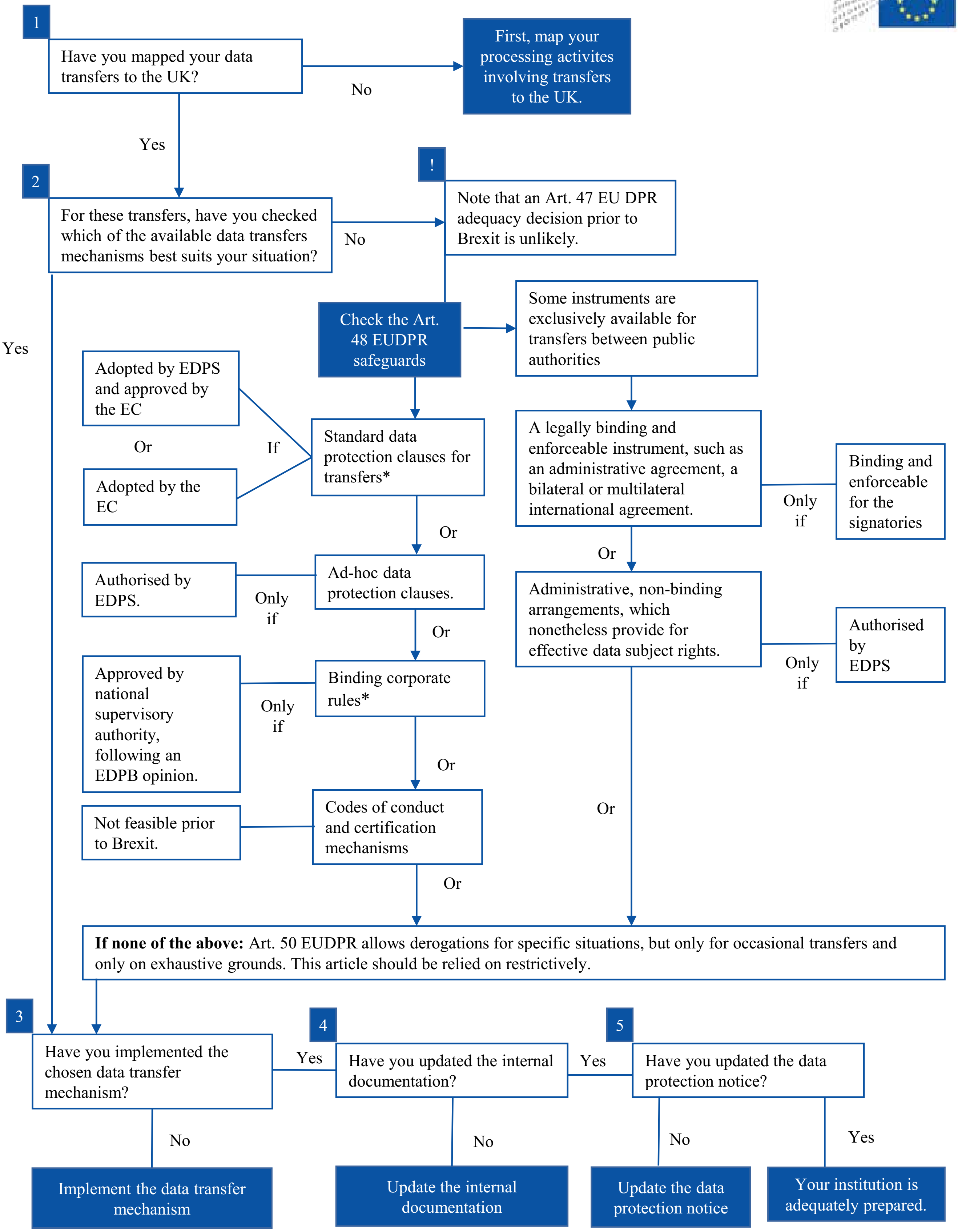
Guiding questions on accuracy

- What could be the consequences for the persons affected of acting on inaccurate information in this process?
- How do you ensure that the data you collect yourself are accurate?
- How do you ensure that data you obtain from third parties are accurate?
- Do your tools allow updates/correction of data where necessary?
- Do your tools allow for consistency checks?

Guiding questions on security

- Do you have a procedure to perform an identification, analysis and evaluation of the information security risks possibly affecting personal data and the IT systems supporting their processing?
- Do you target the impact on people's fundamental rights, freedoms and interests and not only the risks to the organisation?
- Do you take into consideration the nature, scope, context and purposes of processing when assessing the risks?
- Do you manage your system vulnerabilities and threats for your data and systems?
- Do you have any resources or staff with assigned roles to perform risk assessments?

Flowchart: data transfers in the context of Brexit



1 Have you mapped your data transfers to the UK?

No → First, map your processing activites involving transfers to the UK.

Yes ↓

2 For these transfers, have you checked which of the available data transfers mechanisms best suits your situation?

No → ! Note that an Art. 47 EU DPR adequacy decision prior to Brexit is unlikely.

Check the Art. 48 EUDPR safeguards

Some instruments are exclusively available for transfers between public authorities

A legally binding and enforceable instrument, such as an administrative agreement, a bilateral or multilateral international agreement. Only if Binding and enforceable for the signatories

Or

Administrative, non-binding arrangements, which nonetheless provide for effective data subject rights. Only if Authorised by EDPS

Or

Standard data protection clauses for transfers* If Adopted by EDPS and approved by the EC Or Adopted by the EC

Or

Ad-hoc data protection clauses. Only if Authorised by EDPS.

Or

Binding corporate rules* Only if Approved by national supervisory authority, following an EDPB opinion.

Or

Codes of conduct and certification mechanisms — Not feasible prior to Brexit.

Or

If none of the above: Art. 50 EUDPR allows derogations for specific situations, but only for occasional transfers and only on exhaustive grounds. This article should be relied on restrictively.

Yes

3 Have you implemented the chosen data transfer mechanism?

No → Implement the data transfer mechanism

Yes →

4 Have you updated the internal documentation?

No → Update the internal documentation

Yes →

5 Have you updated the data protection notice?

No → Update the data protection notice

Yes → Your institution is adequately prepared.

* Binding corporate rules and standard contractual clauses (adopted by the EC) under the old Directive 95/46 are still valid, but will need to be updated over time in line with the GDPR. In any case, before using old EC standard contractual clauses you should make sure to adapt them to Regulation (EU) 2018/1725 [EUDPR].

Powers of the EDPS under Regulation (EU) 2018/1725
(EU institutions Data Protection Regulation - EUDPR)

Article 58 Powers

1. The European Data Protection Supervisor shall have the following **investigative powers**:

- to **order** the controller and the processor **to provide any information** it requires for the performance of his or her tasks;
- to carry out **investigations** in the form of data protection audits;
- to **notify** the controller or the processor of an **alleged infringement** of this Regulation;
- to **obtain**, from the controller and the processor, **access to all personal data and to all information necessary** for the performance of his or her tasks;
- to **obtain access to any premises** of the controller and the processor, including to **any data processing equipment and means**, in accordance with Union law.

2. The European Data Protection Supervisor shall have the following **corrective powers**:

- to **issue warnings** to a controller or processor that **intended processing operations are likely to infringe** provisions of this Regulation;
- to **issue reprimands** to a controller or a processor where **processing operations have infringed** provisions of this Regulation;
- to **refer matters** to the controller or processor concerned and, if necessary, to the European Parliament, the Council and the Commission;
- to **order** the controller or the **processor to comply with the data subject's requests** to exercise his or her rights pursuant to this Regulation;
- to **order** the controller or processor **to bring processing operations into compliance** with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- to **order** the controller to **communicate a personal data breach** to the data subject;
- to **impose a temporary or definitive limitation** including a **ban on processing**;
- to **order the rectification or erasure of personal data or restriction of processing** pursuant to Articles 18, 19 and 20 and the **notification of such actions to recipients** to whom the personal data have been disclosed pursuant to Article 19(2) and Article 21;

- to **impose an administrative fine pursuant** to Article 66 in the case of non-compliance by an EUI with one of the measures referred to in points (d) to (h) and (j) of this paragraph, depending on the circumstances of each individual case;

- to **order the suspension of data flows** to a recipient in a Member State, a country outside of the EU or to an international organisation.

3. The European Data Protection Supervisor shall have the following **<u>authorisation and advisory powers:</u>**

- to **advise data subjects** on exercising their rights;

- to **advise** the controller in accordance with the **prior consultation** procedure referred to in Article 40, and in accordance with Article 41(2);

- to **issue**, on his or her own initiative or on request, **opinions** to EUIs and to the public on any issue related to the protection of personal data;

- to **adopt standard data protection clauses** referred to in Article 29(8) and in point (c) of Article 48(2);

- to **authorise contractual clauses** referred to in point (a) of Article 48(3);

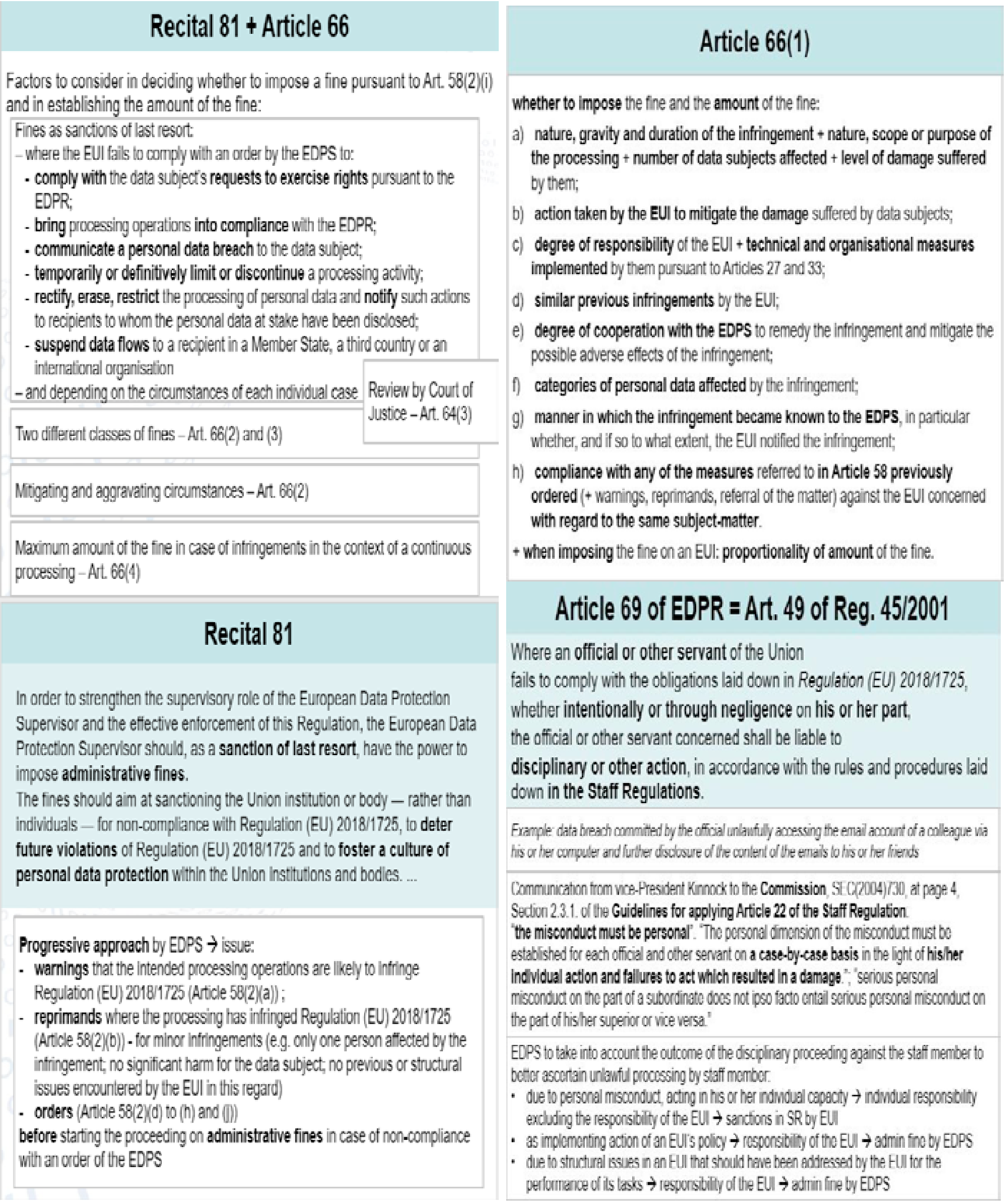
- to **authorise administrative arrangements** referred to in point (b) of Article 48(3);

- to **authorise processing operations** pursuant to implementing acts adopted under Article 40(4).

4. The European Data Protection Supervisor shall have the **power to refer the matter to the Court of Justice** under the conditions provided for in the Treaties and to **intervene in actions brought before the Court of Justice**.

5. The **exercise of the powers** conferred on the European Data Protection Supervisor pursuant to this Article shall be **subject to appropriate safeguards**, including effective judicial remedies and due process, set out in EU law.

Administrative fines and sanctions, under EUDPR



Recital 81 + Article 66

Factors to consider in deciding whether to impose a fine pursuant to Art. 58(2)(i) and in establishing the amount of the fine:

Fines as sanctions of last resort:

– where the EUI fails to comply with an order by the EDPS to:

- **comply with** the data subject's **requests to exercise rights** pursuant to the EDPR;
- **bring** processing operations **into compliance** with the EDPR;
- **communicate a personal data breach** to the data subject;
- **temporarily or definitively limit or discontinue** a processing activity;
- **rectify, erase, restrict** the processing of personal data and **notify** such actions to recipients to whom the personal data at stake have been disclosed;
- **suspend data flows** to a recipient in a Member State, a third country or an international organisation

– and depending on the circumstances of each individual case

Review by Court of Justice – Art. 64(3)

Two different classes of fines – Art. 66(2) and (3)

Mitigating and aggravating circumstances – Art. 66(2)

Maximum amount of the fine in case of infringements in the context of a continuous processing – Art. 66(4)

Recital 81

In order to strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a **sanction of last resort**, have the power to impose **administrative fines**.

The fines should aim at sanctioning the Union institution or body — rather than individuals — for non-compliance with Regulation (EU) 2018/1725, to **deter future violations** of Regulation (EU) 2018/1725 and to **foster a culture of personal data protection** within the Union institutions and bodies. ...

Progressive approach by EDPS → issue:

- **warnings** that the intended processing operations are likely to infringe Regulation (EU) 2018/1725 (Article 58(2)(a)) ;
- **reprimands** where the processing has infringed Regulation (EU) 2018/1725 (Article 58(2)(b)) - **for minor infringements** (e.g. only one person affected by the infringement; no significant harm for the data subject; no previous or structural issues encountered by the EUI in this regard)
- **orders** (Article 58(2)(d) to (h) and (j))

before starting the proceeding on **administrative fines** in case of non-compliance with an order of the EDPS

Article 66(1)

whether to impose the fine and the **amount** of the fine:

a) **nature, gravity and duration of the infringement + nature, scope or purpose of the processing + number of data subjects affected + level of damage suffered** by them;

b) **action taken by the EUI to mitigate the damage** suffered by data subjects;

c) **degree of responsibility** of the EUI + **technical and organisational measures implemented** by them pursuant to Articles 27 and 33;

d) **similar previous infringements** by the EUI;

e) **degree of cooperation with the EDPS** to remedy the infringement and mitigate the possible adverse effects of the infringement;

f) **categories of personal data affected** by the infringement;

g) **manner in which the infringement became known to the EDPS**, in particular whether, and if so to what extent, the EUI notified the infringement;

h) **compliance with any of the measures** referred to **in Article 58 previously ordered** (+ warnings, reprimands, referral of the matter) against the EUI concerned **with regard to the same subject-matter**.

+ **when imposing** the fine on an EUI: **proportionality of amount** of the fine.

Article 69 of EDPR = Art. 49 of Reg. 45/2001

Where an **official or other servant** of the Union fails to comply with the obligations laid down in *Regulation (EU) 2018/1725*, whether **intentionally or through negligence** on **his or her part**, the official or other servant concerned shall be liable to **disciplinary or other action**, in accordance with the rules and procedures laid down **in the Staff Regulations**.

Example: data breach committed by the official unlawfully accessing the email account of a colleague via his or her computer and further disclosure of the content of the emails to his or her friends

Communication from vice-President Kinnock to the **Commission**, SEC(2004)730, at page 4, Section 2.3.1. of the **Guidelines for applying Article 22 of the Staff Regulation**. "**the misconduct must be personal**". "The personal dimension of the misconduct must be established for each official and other servant on **a case-by-case basis** in the light of **his/her individual action and failures to act which resulted in a damage**."; "serious personal misconduct on the part of a subordinate does not ipso facto entail serious personal misconduct on the part of his/her superior or vice versa."

EDPS to take into account the outcome of the disciplinary proceeding against the staff member to better ascertain unlawful processing by staff member:

- due to personal misconduct, acting in his or her individual capacity → individual responsibility excluding the responsibility of the EUI → sanctions in SR by EUI
- as implementing action of an EUI's policy → responsibility of the EUI → admin fine by EDPS
- due to structural issues in an EUI that should have been addressed by the EUI for the performance of its tasks → responsibility of the EUI → admin fine by EDPS

EUDPR - Infringements

Category 1 Infringements maximum fine of 25 000 EUR per infringement and of 250 000 EUR per year	***Category 2 Infringements*** maximum fine of 50 000 EUR per infringement and of 500 000 EUR per year
Infringements for which fining is explicitly set out in Art. 66(2) of the EUDPR	**Infringements for which fining is explicitly set out in Art. 66(3) of the EUDPR**
Art. 8 - Conditions applicable to a child's consent in relation to information society services	**Art. 4** - Principles relating to processing of personal data
Art. 12 - Processing which does not require identification	**Art. 5 -** Lawfulness of processing
Art. 27 - Data protection by design and by default	**Art. 7 -** Conditions for consent
Art. 28 - Joint controllers	**Art. 10** - Processing of special categories of personal data
Art. 29 - Processor	**Art. 14 -** Transparent information, communication and modalities for the exercise of the rights of the data subject
Art. 30 - Processing under the authority of the controller or processor	**Art. 15 -** Information to be provided where personal data are collected from the data subject
Art. 31 - Records of processing activities	**Art. 16 -** Information to be provided where personal data have not been obtained from the data subject
Art. 32 - Cooperation with the European Data Protection Supervisor	**Art. 17 -** Right of access by the data subject
Art. 33 - Security of processing	**Art. 18 -** Right to rectification
Art. 34 - Notification of a personal data breach to the European Data Protection Supervisor	**Art. 19 -** Right to erasure ('right to be forgotten')
Art. 35 - Communication of a personal data breach to the data subject	**Art. 20 -** Right to restriction of processing
Art. 39 - Data protection impact assessment	**Art. 21 -** Notification obligation regarding rectification or erasure of personal data or restriction of processing
Art. 40 - Prior consultation	**Art. 22 -** Right to data portability
Art. 43 - Designation of the data protection officer	**Art. 23 -** Right to object
Art. 44 - Position of the data protection officer	**Art. 24 -** Automated individual decision-making, including profiling
Art. 45 - Tasks of the data protection officer	**Art. 46 -** General principle for transfers
	Art. 47 - Transfers on the basis of an adequacy decision
	Art. 48 - Transfers subject to appropriate safeguards
	Art. 49 - Transfers or disclosures not authorised by Union law
	Art. 50 - Derogations for specific situations
Infringements for which fining is not explicitly set out in Art. 66(2) or (3), but could be sanctioned in line with Art. 66(1) as failure to comply with order under Art. 58(2)(e) of the EUDPR	**Infringements for which fining is not explicitly set out in Art. 66(2) or (3), but could be sanctioned in line with Art. 66(1) as failure to comply with order under Art. 58(2)(e) of the EUDPR**
Rec (49) EUDPR in connection with Art. 42 GDPR - Certification of EUI	**Art. 6 -** Processing for another compatible purpose
Art. 26 - Responsibility of the controller	**Rec (21) in connection with Art. 5 -** Transmission of personal data within the same Union institution or body and the recipient is not part of the controller, or to other Union institutions or bodies
Art. 37 - Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment	**Art. 9 -** Transmissions of personal data to recipients established in the EU other than Union institutions and bodies
Art. 38 - Directories of users	**Art. 11 -** Processing of personal data relating to criminal convictions and offences
	Art. 13 - Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
	Art. 25 - Restrictions
	Art. 36 - Confidentiality of electronic communications

EDPS

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor