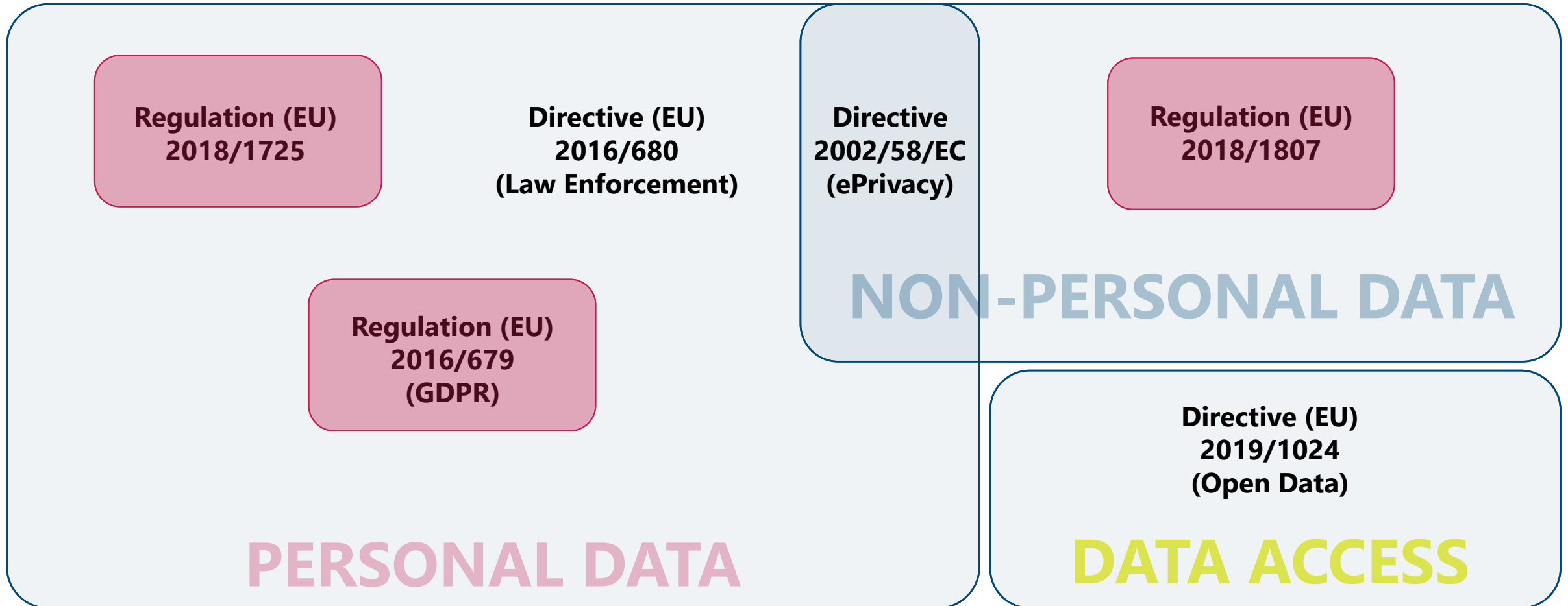


How much anonymisation is needed? A legal perspective

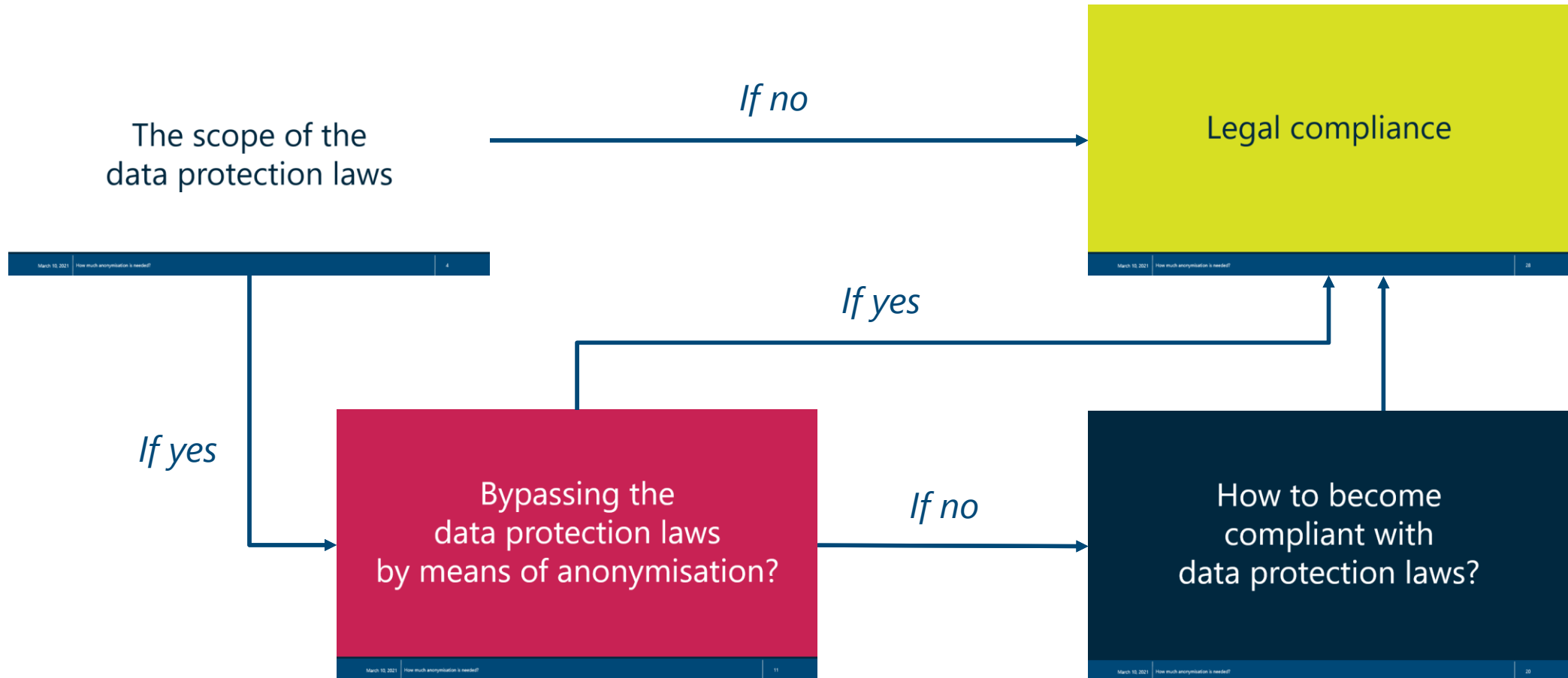
5th ELRC Conference – March 10, 2021

Jonas Baumann & Dr. Andreas Sasing

The legal framework for data processing in the EU



Agenda



The scope of the data protection laws

The scope of the data protection laws

Personal Data

Article 4 (1) GDPR

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly [...]

The scope of the data protection laws

Examples of personal data

- Andreas Sasing
- jonas.baumann@uni-saarland.de

What about an IP address?

- 134.96.60.167

Examples of non-personal data

- 12°C
- 156 meters
- S26 10 54.9 E27 59 53.9
(= GPS Coordinates: University of Johannesburg APK Campus)
- Volkswagen AG

The scope of the data protection laws

When is a person “identifiable”?

- Identification (regularly) requires additional information/knowledge
- What information needs to be taken into account?
 - objective approach – “entire world knowledge”
 - subjective approach – “knowledge available to the data controller”

The scope of the data protection laws

ECJ, Judgment from 19.10.2016, C-582/14 (*Breyer v Germany*)

“[...] to determine whether a person is identifiable, account should be taken of all the **means likely reasonably to be used either by the controller or by any other person** to identify the said person”. (para. 42)

“ [...], that would **not be the case** if the identification of the data subject was **prohibited by law or practically impossible** on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that **the risk** of identification appears in reality **to be insignificant.**” (para. 46)

The scope of the data protection laws

ECJ, Judgment from 19.10.2016, C-582/14 (*Breyer v Germany*)

- Extensive interpretation of “personal data”
- (Implicit) rejection of the traditional approaches (both *objective* and *subjective*)
- IP addresses can be personal data

The scope of the data protection laws

Interim conclusion

- Personal data is always context-related
- Personal data is a binary concept



Bypassing the data protection laws by means of anonymisation?

Bypassing data protection law by means of anonymisation?

ECJ, Judgment from 19.10.2016, C-582/14 (*Breyer v Germany*)

“ [...], that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact **that it requires a disproportionate effort** in terms of time, cost and man-power, so **that the risk of identification appears in reality to be insignificant.**” (para. 46)

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Example: Anonymisation of court judgments (I)

Information required for
the legal reasoning

TRANSPARENCY




Information not be
disclosed to the public

PRIVACY

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Example: Anonymisation of court judgments (II)



Court of Justice of the European Union
PRESS RELEASE No 96/18
Luxembourg, 29 June 2018

Press and Information

From 1 July 2018, requests for preliminary rulings involving natural persons will be anonymised

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Example: Anonymisation of court judgments (III)

- Recently in Germany
 - Judgment of the *Bundesgerichtshof* was published two years after the ruling
 - In the meantime: Three (!) court decisions addressed the question whether the “anonymised” version of the judgment could be published

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Example: Anonymisation of court judgments (IV)

- How anonymised was the decision?
 - Plaintiff is a professor for civil law & other subjects
 - Contributes to the same volume of a prominent civil law textbook as his wife
 - Parts of the title of the textbook were mentioned
 - Latest edition of the textbook was published in 2013
 - Initials and title of the editor in chief were mentioned ("Professor M.")

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Art. 2 (2) Regulation (EU) 2018/1807

In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.

⇒ Personal data “infects” the whole data set

⇒ One “infected” data set “infects” the whole database

Bypassing data protection law by means of anonymisation?

How much anonymisation is required?

Art. 29 Data Protection Working Party – WP 216 (p. 10)

[...] It must be clear that 'identification' not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, linkability and inference. Furthermore, for data protection law to apply, it does not matter what the intentions are of the data controller or recipient. As long as the data are identifiable, data protection rules apply.

Bypassing data protection law by means of anonymisation?

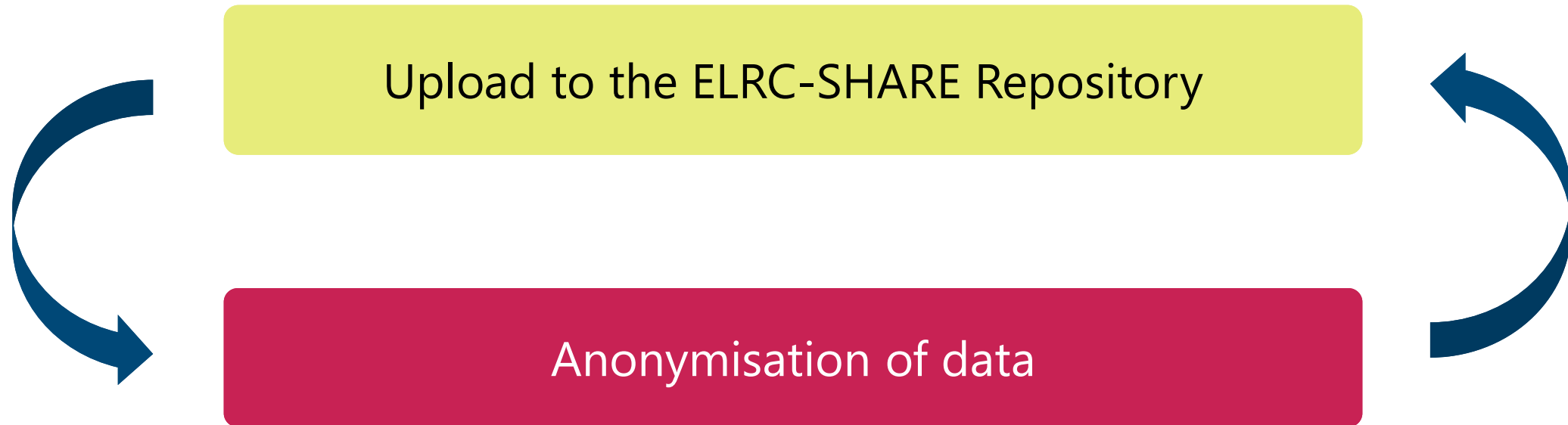
Interim Conclusion

- Bypassing data protection laws require an anonymisation of all data sets in the repository
- Contextual information in single data sets can render a person “identifiable”
- “Swapping” of personal information alone is not sufficient to bypass the application of data protection law
- Application of data protection law cannot be excluded *ex ante*

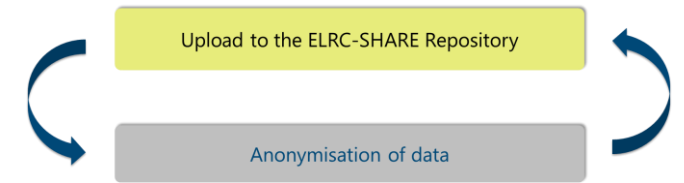
How to become compliant with data protection laws?

How to become compliant?

Relevant processing



How to become compliant?



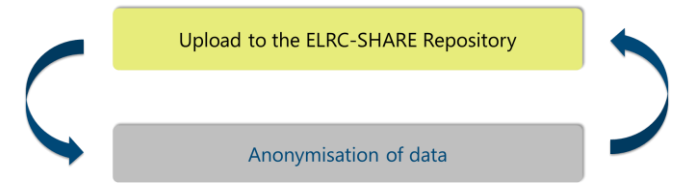
Legal basis for uploading personal data

- *Example: Uploading of ECJ decisions into the European Court Reports*

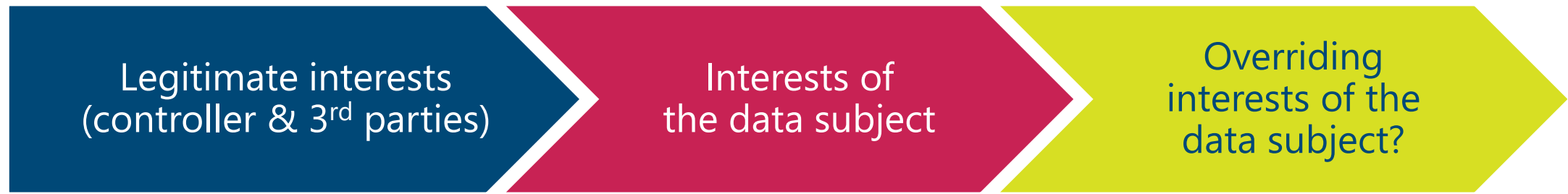
Art. 92 Consolidated version of the Rules of Procedure of the Court of Justice of 25 September 2012

A notice containing the date and the operative part of the judgment or order of the Court which closes the proceedings shall be published in the Official Journal of the European Union.

How to become compliant?

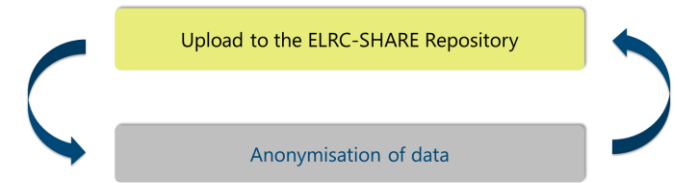


Legal basis for uploading personal data – private donors



- Legitimate interests include: economic interests, efficient AI training, freedom of information, public repository for training data
 - Anonymisation mitigates the risks of the data subject
- ⇒ Uploading to the ELRC-SHARE Repository can be based on Art. 6 (1) (f) GDPR

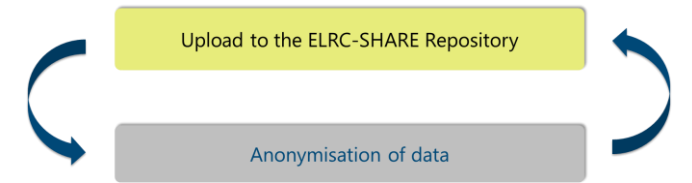
How to become compliant?



Legal basis for uploading personal data – public donors

- Legitimate interest: no legal basis for contributing to the ELRC-SHARE Repository for public authorities
- Legal basis for the data upload is required
- Provisions of the Regulation 1/1958 (consolidated version from 1.7.2013)?
- Open Data Directive?
 - Does the provision even provide a legal basis for such an upload?
 - Is the data upload to the ELRC-SHARE Repository “necessary” to fulfil transparency requirements?

How to become compliant?



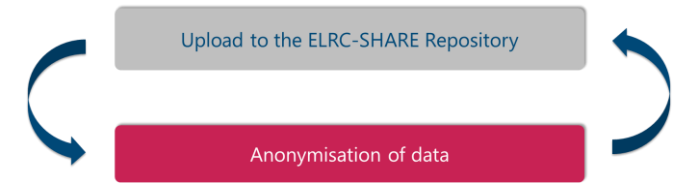
Legal basis for uploading personal data

“Problem” within the European Data Protection Law framework:

There is no legal basis that explicitly permits the processing of personal data (especially the submission to an open repository) for the purpose of training AI systems.



How to become compliant?



Legal basis to anonymise data

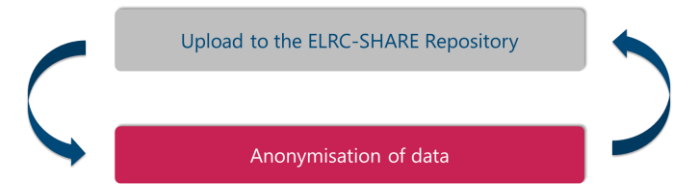
- Obligation to implement technical and organisational measures

Art. 32 (1) GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller [...] shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, **including inter alia** as appropriate:

(a) the pseudonymisation and encryption of personal data;

How to become compliant?



Legal basis to anonymise data

Interim Conclusion:

Anonymisation of personal data can be based on the obligation to implement technical and organisational measures according to Art. 32 (1) GDPR

...but...

this provision can only be considered as a legal basis for anonymisation if there is a lawful “main processing” (in our case: upload).

Legal compliance

Legal compliance

- “Swapping” of personal information alone is not sufficient to bypass the application of data protection laws
- Anonymisation appears to be an effective way to protect the interests of data subjects
- Solution for public donors: Regulation of the processing of personal data relating to the training of AI systems could provide legal certainty

Thank you!

Questions?

Jonas Baumann, LL.M. (University of Johannesburg)

jonasb@uj.ac.za

Dr. Andreas Sasing

andreas.sasing@uni-saarland.de