Page 28- “Public interest or exercise of official authority (Article 6(1)(e) GDPR)

57. (…) For example, Union and MS law may authorise a controller to conduct scientific research in a certain field in the public interest, without necessarily specifying how the research is to be undertaken.

58. Relying on performance of a task carried out in the public interest, or exercise of official authority, as a legal basis is not limited to public entities conducting scientific research. Private entities may also rely on that legal basis, if the legal act covers their activities”

Page 32- “4.4.3 Derogations laid down in Union or MS law (Article 9(2)(g), (i) and (j) GDPR)

73. Controllers may rely on derogations to the prohibition of processing of special categories of data provided for by Union or MS law, pursuant to Article 9(2)(g), (i) and (j) of the GDPR, when processing personal data for scientific research purposes.115 Such laws must “respect the essence of the fundamental rights and observe the principle of proportionality”116. To fulfil the principle of proportionality, the laws must – inter alia – provide for suitable and specific measures, to safeguard the fundamental rights and interests of the data subject, to be adopted by the controller117.”

Comments:

The use of Article 6(1)(e) (public interest/official authority) together with the derogations under Article 9(2)(g), (i), and (j) for scientific research introduces some data protection risks, such as:

- **Lack of specificity in the legal basis:** laws may authorise processing for “scientific research in the public interest” without clearly defining the scope, purposes, or limits of the processing. This may create a risk of overly broad interpretation, reducing predictability for data subjects and potentially undermining the principles of lawfulness, fairness, and transparency. As a result, controllers may process more data than necessary or use it in ways that were not originally foreseeable.
- **Misuse by private entities:** since private organisations can rely on Article 6(1)(e) when permitted by law, there is a risk that the notion of “public interest” may be stretched to cover activities that are partially commercial or self-serving. This increases the likelihood of function creep, where data collected for research is gradually reused for other purposes, eroding trust and compliance.
- **Proportionality**, particularly under Article 9 derogations. Although the GDPR requires that national or EU laws respect proportionality, in practice these laws may allow the processing of large volumes of special category data without sufficiently

strict limits. This might create a risk of violating the data minimisation principle, especially where necessity is not rigorously assessed.

- **Special categories of data** (such as health, genetic, or biometric data)**:** may introduce inherently high risks to individuals' rights and freedoms. Even where pseudonymisation is applied, there remains a significant risk of reidentification, particularly in research contexts involving rich datasets. In addition, misuse or breaches involving such data can lead to discrimination or serious personal harm.
- **Insufficient implementation of safeguards:** while the law may mandate measures such as pseudonymisation and access controls, these safeguards could applied inconsistently or inadequately. Weak technical and organisational measures can result in unauthorised access, data leakage, or misuse.
- **Non-compliance with transparency obligations:** Even when derogations apply, controllers must still provide information where data is collected directly from the data subject. Organisations may incorrectly assume they are exempt and fail to provide adequate notice, leading to breaches of Articles 13 and 14 GDPR.
- **Incompatible reuse of data: s**cientific research benefits from some flexibility under the GDPR, but this can lead to overly broad interpretations, where data is reused for new projects without proper compatibility assessments. This threatens the principle of purpose limitation.
- **Governance and accountability risk**. these legal bases require a high level of legal, technical, and organisational maturity. Without proper internal policies, documentation, and oversight (e.g. DPIAs, records of processing), organisations may fail to demonstrate compliance, exposing themselves to regulatory and reputational consequences.