CYBERSECURITY IN BIOBANKING: THE LEGAL FRAMEWORK PROTECTING AND SECURING DATA

ALMEIDA, Catarina[(1)], FORGÓ, Nikolaus[(1)], HENNE, Theresa[(1)] and MARQUEZ, Rodessa May[(1)]

1) Department of Innovation and Digitalisation in Law, Faculty of Law, University of Vienna, Austria

Partner of the BBMRI.at Project, funded by the Federal Ministry for Education, Science and Research, grant number 2023-0.752.780.

Cybersecurity Incidents in Biobanking

Malicious

Non-malicious

Examples:

- Unauthorized data access;
- Data leaks;
- Data manipulation, corruption and deletion / loss;
- Improper data deletion (post-storage);
- Ransomware and espionage;
- Data misuse;
- Data linking and reversal of pseudonymisation;
- Biosafety / biosecurity hazards.

→

1. Data Security is a paramount ELSI concern;

2. Existing governance instruments, both binding and non-binding, highlight the importance of data security.

EU & AUSTRIAN LEGAL INSTRUMENTS FOR DATA SECURITY & THEIR KEY ELEMENTS

GENERAL DATA PROTECTION REGULATION (GDPR)

1. Applicable to personal data processing operations (Art 1).
2. Data integrity and confidentiality as key principle of personal data processing (Art 5(1)(f)): protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
3. Implementation of technical and organizational measures appropriate to the risks of the personal data processing, such as pseudonymisation and encryption (Art 32).
4. Includes compensation and liability for violations of Art 32 (Art 82).
5. Creates personal data breach notification and communication procedures (Arts 33 and 34).

NETWORK AND INFORMATION SYSTEMS (NIS II) DIRECTIVE

1. Cybersecurity legal framework applicable to medium and large public or private entities operating in 18 critical sectors (Art 1), including both health (high criticality sector – essential entities) and research (other critical sectors – important entities) (Annexes 1 and 2).
2. Applicability to biobanks depends on their size and scope and is unlikely. However, hospitals and universities (in which often biobanks are integrated), may fall under the scope of the NIS II Directive.
3. National transposition of the Directive will also dictate the terms in which biobanks are affected.

EUROPEAN HEALTH DATA SPACE (EHDS) REGULATION

1. Applicable to biobanks who are electronic health data holders or users (Art 1 and 2). Biobank health data must be made available for secondary use (Art 51(1)(q)).
2. For secondary use, data is shared in an anonymised or pseudonymised form (Art 66).
3. Data for secondary use is shared through a secure processing environment (SPE) with security measures (Art 73), such as restriction of access and minimisation of the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the SPE.
4. Further specifications for SPEs will be determined by the EU Commission through implementing acts (Art 73(5)).

AUSTRIAN NATIONAL LAW

1. Data Protection Act (*Datenschutzgesetz*, 'DSG')

   For scientific research processing purposes:
   - Special provisions for data confidentiality (if processing concerns special categories of personal data) (§ 7);
   - Data pseudonymisation, anonymisation and encryption measures;
   - National implementation of the GDPR provisions for data breaches (§ 55 and 56).

2. Research Organisation Act (*Forschungsorganisationsgesetz*, 'FOG')

   - Data secrecy principle (§ 2d(1));
   - Prohibition of publication of personal identifiers (§ 2d(1)).

Thought-provoking discussion points:

Is the existing legal framework for data security satisfactory and sufficient?

Does data security depend on the available legal framework, or more on the individual adherence and adoption of best practices by each biobank and biobank researcher?

Is there need for more data security awareness?

References:

- Kaya Akyüz and others, 'Biobanking and risk assessment: a comprehensive typology of risks for an adaptive risk governance' (2021) 17 Life Sci Soc Policy 10
- Ramez Alkhatib and Karoline I Gaede, 'Data Management in Biobanking: Strategies, Challenges, and Future Directions' (2024) BioTech 34
- Cédric Burton, 'Article 32. Security of Processing' in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds) The EU General Data Protection Regulation (GDPR) (Oxford University Press 2020) 730.

Federal Ministry Women, Science and Research Republic of Austria

Funded by the Austrian Federal Ministry of Women, Science and Research (BMFWF)
Grant number: 2023-0.752.780 (2023-2028)