



EUROPE BIOBANK WEEK CONGRESS 19-22 MAY 2026

POSTER SESSIONS

Abstracts

Produced by the Europe Biobank Week Programme Committee and BBMRI-ERIC's
Department of Outreach, Education and Communications

497: Cybersecurity in Biobanking: the
Legal Framework protecting and securing
data

Authors:

Catarina Almeida, 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.

Nikolaus Forgó, 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.

Theresa Henne, 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.

Rodessa May Marquez, 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.

Abstract ID: 497

*Topic: 6B: Secure, Fair and Smart: Best Practices
for Biobank Data Integration*

Presenter Name: Catarina Almeida

*Keywords: Cybersecurity, Data Protection, Data
security, European Union, Legal Framework*

Biobanks operate under the premise of data sharing, including personal and sensitive personal data, as defined by the GDPR. The GDPR provides key mechanisms and features for safeguarding personal data, such as the obligation, in certain circumstances, to conduct data protection impact assessments and implement technical and organizational measures to secure the data. The framework for personal data sharing will become more complex with the advent of the implementation of the EHDS Regulation. Cyberattacks on health infrastructures show that healthcare and research systems face growing digital threats. Biobanking infrastructures are complex organizational structures, with a wide network of actors, which may conceal cybersecurity vulnerabilities. Therefore, the field of cybersecurity is increasingly prominent and compliance with legal acts such as the NIS 2 Directive are critical in this instance, and affect hospitals and research institutions, in the prevention and mitigation of (malicious and non-malicious) cyber incidents. Legal desk research undertaken by BBMRI.at's WP2, *inter alia* resorting to published materials on the topic.

The current regulatory framework for data protection and information security at both national and EU levels will be analyzed. This is relevant to ensure the sustainability and resilience of biobanks long term, ensuring data quality, storage and preservation compatible with the need for data sharing and secondary use in scientific research.

The focus of the poster will be on the data protection and security challenges encountered by biobanks and the legal framework currently in place to protect and secure data, from the GDPR, EHDS and NIS 2 Directive.