Syllabus
Course description

Course title	**Cybersecurity and digital privacy**
Course code	27513
Scientific sector	IUS/01 – GIUR-01/A
Degree	Master in Data Analytics for Economics and Management
Semester and academic year	1st semester a.y. 2025/2026
Year	2nd study year
Credits	6
Modular	No

Total lecturing hours	48
Total lab hours	/
Total exercise hours	/
Attendance	Suggested, but not required
Prerequisites	None
Course page	Master in Data Analytics for Economics and Management / Free University of Bozen-Bolzano (unibz.it)

Specific educational objectives	The course deals with the main legal issues on personal and non-personal data processing and the risk management that a cyber-company faces in the current European regulatory framework. In the first part of the course personal and non-personal data processing regulations will be studied. The GDPR's main provisions will be described, and then how the GDPR addresses the rules governing data processing and the duties cast upon controllers and processors. The role and obligations of Data Protection Officers (DPO) are dealt with. The second part of the course focuses on cybersecurity. After the description of the main threats and vulnerabilities of networks, it focuses on the best practices and rules used to tackle them. It analyses the NIS Directive and the Cybersecurity Act in force into the European Union. It concludes with the discussion about how these rules are tailored within specific industries. The comparative perspective among the EU legal model with the US legal model and the Chinese legal model of data processing and protection will be explored. The international level of rules formation in the field is also taken into account.

Lecturers	20 hours – Laura Valle
	Laura Valle / Libera Università di Bolzano (unibz.it)
	28 hours – Laura Greco
	Laura Greco / Free University of Bozen-Bolzano
Scientific sector of the lecturers	IUS/01 – GIUR-01/A
Teaching language	English
Office hours	Please refer to the lecturers' timetables
Lecturing assistant	/
Teaching assistant	/
Office hours	/
List of topics covered	Part I. European Data Protection Law: General provisions; Personal data and non-personal data; Principles and rights related to data processing and data subjects; Controller and processor; Security of personal data; Data protection officer; Personal data protection and consequences of the breaches of law; data protection and cybersecurity protection and AI.
	Part II. Cybersecurity: threats and vulnerabilities; best practices, standards and rules; the NIS EU Directive of 2016; the Cybersecurity Act of 2017; The EU Directive NIS of 2022, and the Italian law n. 90/2024; Cybersecurity Governance; industry specific cybersecurity rules; the use of the models of law n. 231/2001 and of ISO 9001.
	Comparative perspectives among different legal models. Development of rules and practices at the international level.
Teaching format	The course adopts a blended, student-centred approach that emphasises problem-based learning and active engagement. A portion of the lecture content is made available online in advance, allowing students to explore key concepts independently and at their own pace before attending class. This preparatory work enables in-person sessions to focus on the application of knowledge through real-world problems, collaborative activities, and guided discussions — fostering critical thinking and deeper learning. The course is fully aligned with the principles of the Italian Universities Digital Hub (EDUNEXT) initiative (https://edunext.eu), which promotes the integration of digital resources and active learning strategies within university teaching.

Learning outcomes	Knowledge and understanding:
	- Knowledge and understanding of the legal sources relating to the fields of the course at the national, European and at the international level. - Knowledge and understanding of the legal problems connected to data processing. Applying knowledge and understanding: - Ability to search and use of the interested sources of law at the national, European, and international contexts. - Ability to analyse case studies emerging in practice, and to apply the appropriate concepts of the interested rules of law. - Ability to support firms and public entities about the legal issues object of the lecture course. Making judgments - Ability to find, read and evaluate new and updated data, rules of law, professional and scientific publications, as well as news in journals, newspapers, media. Communication skills: - Ability to produce the legal notions learned in the course using an appropriate scientific and professional language. Learning skills: - Development of skills of interpretation and application of the legal rules in the field interested.

Assessment	The course grade will be based on the final written exam that include 3 general questions with 3-4 sub-questions.
Assessment language	English
Evaluation criteria and criteria for awarding marks	Relevant for the assessment of the written exam: clarity of the answers, mastery of language (knowledge of the legal technical language, and grammatical and logic mastery of language), ability to summarize, evaluate, and establishing relationships between topics.

Required readings	- *Data protection in context: between privacy and AI*, ed. by E. Longo, A. Pin, F. Viglione, Giuffré, Milano, 2025. - More in-depth materials on cybersecurity topics will be indicated at the beginning of the lectures course. The parts to prepare for the exam will be indicated in a detailed syllabus on Teams.

Supplementary readings	/