COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Course unit code
DATA PROTECTION AND PRIVACY LAW IN THE AGE OF AI	

Lecturer(s)	Department(s)
Coordinator: senior lect. dr. Paulius Jurčys **Other(s):**	Department of Public Law, Faculty of Law, Vilnius University; Room 411, Building 1, Saulėtekio al. 9, LT-10222, Vilnius, tel. (85)2366175, e-mail: vtkatedra@tf.vu.lt

Study cycle	Type of the course unit (module)
Second	Compulsory (Track – Tech Law)

Mode of delivery	Course unit delivery period	Language (s) of instruction
Blended	Spring semester	English

Requirements for students	
Pre-requisites: none	**Co-requisites (if any):** none

Number of credits allocated	Total student's workload	Contact hours	Self-study hours
5	133	32	101

Purpose of the course unit (module): programme competences to be developed		
The aim of the course is to provide students with comprehensive knowledge of data privacy and data protection law from a distinctly human-centric perspective; to develop understanding and abilities to analyse and apply the core principles and foundations of data protection and privacy law in the EU, the United States (California and a few selected other federal states) with the emphasis on data-driven and agentic AI context; and competencies to deliver legal recommendations on related practical issues. Students gain abilities to critically analyse the shift from enterprise-centric data architectures to user-held, private-by-default, human-centric data models, and assess how personal AI, AI twins, AI agents, synthetic identities and platform automation challenge established legal categories, as well as abilities to use different AI tools and build AI literacy as an essential professional skill.		
Learning outcomes of the course unit (module)	**Teaching and learning methods**	**Assessment methods**
Students will gain a systematic and practical understanding of core principles of personal data protection and privacy law, including privacy as a human right, data subject rights, consent, transparency, purpose limitation, data minimisation, security, accountability, portability and remedies.	Lectures and practical sessions based on discussion, case analysis, doctrinal analysis, comparative legal analysis and guided use of AI tools for preparation and reflection.	Take-home examination, student presentations, preparation and active participation.
Students will be able to compare and apply EU, US and several federal state approaches to privacy and data protection, including GDPR, CCPA/CPRA, sectoral and tort-based privacy frameworks, case law and regulatory practice.	Problem-based and comparative learning; analysis of legal materials, scholarly texts, court decisions, regulatory guidance and current examples from technology markets.	Take-home examination, presentation, discussion and issue-spotting exercises.
Students will understand the distinction between enterprise-centric and human-centric data models and will be able to explain how user-held data, personal data vaults, private-by-default architectures and local AI systems may alter control, risk and value.	Lectures, discussions during practical sessions, practical thought experiments, group work and analysis of technological scenarios involving personal AI, AI twins, data portability and data ownership.	Take-home examination and group presentations applying human-centric analysis.
Students will be able identify how traditional privacy and data protection concepts are challenged by AI, including large-scale training data, inference, profiling, digital replicas, synthetic identities, AI agents, scraping, automated decision-making and platform automation.	Case-based learning, discussion of contemporary disputes, analysis of AI-related examples and structured use of AI tools to test the limits of existing legal concepts.	Take-home examination, presentation and class discussion.
Students will develop AI literacy as a professional legal competence: they will learn to use AI tools	Hands-on AI exercises using Paul AI, Goda AI, ChatGPT, Gemini, Perplexity,	Preparation and participation during

critically, compare outputs, verify answers, improve prompts and evaluate legal and ethical implications of AI-assisted research and drafting.	Claude and similar tools; comparative output review and classroom reflection.	classes, presentation and take-home exam reasoning.
Students will be able to formulate legal, policy and design recommendations for data and AI systems that better protect individuals, support autonomy and reduce dependence on extractive data architectures.	Research-based group work, policy analysis, design-thinking exercises, discussion of business and regulatory models, and practical presentation workshops.	Presentation and take-home examination.
Students will be able to communicate clearly using contemporary data privacy, data protection, AI governance and human-centric data terminology, and will be able to translate complex technical and legal issues into practical advice.	Socratic discussion, group presentation, oral feedback, peer learning and practical analysis of real-world data and AI scenarios.	Presentation, class discussion and take-home examination.
Students will be able to productively participate in cross-cultural group activities, discuss their own conclusions and well-grounded arguments in a constructive dialogue, evaluate positions advanced by others, taking into account cultural differences and ethical considerations.	Practical sessions (oral presentations, the analysis of problematic issues, group discussions, case study)	Presentation, class discussion and take-home examination.
Students will be able to critically evaluate their own learning, independently select relevant legal and technical materials, and use AI tools responsibly to support legal judgment.	Independent reading, AI-assisted preparation, reflective discussion and a feedback session after the take-home examination.	Preparation and discussion during classes, take-home examination and post-exam feedback participation.

Content: breakdown of the topics	**Contact hours**							**Self-study: hours and assignments**	
	Lectures	Consultations	Seminars	Practical sessions	Laboratory work	Internship/work	**Contact hours**	**Self-study hours**	**Assignments**
1. Introduction: data privacy in the age of AI; course method; human-centric perspective; AI tools and digital legal skills.	2						**2**	**6**	Read course outline; explore Paul AI/Goda AI and one general AI tool; identify a current privacy/AI issue.
2. Origins and conceptions of privacy; Warren/Brandeis; Solove/Schwartz; privacy as control, dignity, autonomy and social practice; The Great Hack.	2						**2**	**7**	Assigned readings and film; AI-assisted questions on origins and conceptions of privacy and human-centric data.
3. Foundations of privacy law; European human-rights foundations; enterprise-centric approach; core principles; why AI challenges privacy principles.	2						**2**	**7**	Solove/Hartzog; Private-by-Default blog post; Hartzog interview; AI comparison exercise.
4. Data subject rights and human-centric data models: right to be forgotten, access rights, portability, user-held data and personal data vaults.	2						**2**	**7**	Readings, court examples and practical exercise requesting or analysing personal data exports.
5. US privacy law framework; privacy torts; platform power; data extraction; private-by-default as an alternative to surveilled-by-default systems.	2						**2**	**7**	Warren/Brandeis, Prosser, Solove/Hartzog, Private-by-Default and Dario Amodei interview.
6. Data ownership and dominion: personal data as value, asset and identity; data ownership debates; data containers and personal AI systems.	2						**2**	**7**	Will.i.am article; short data ownership blog post; longer data ownership law review article; multi-tool AI comparison exercise.

7. Data portability, AI twins and synthetic identities: portability revisited, digital replicas, fictional-character replicas and human-centric networks.	2						**2**	**7**	Data Portability Guidelines; Data Portability Revisited; Who Owns My AI Twin?; Reid Hoffman video; AI comparison exercise.
8. Agentic AI and platform access: AI agents, scraping, Amazon v. Perplexity, personal assistants, consent, terms of use and the limits of existing doctrine.	2						**2**	**7**	Amazon v. Perplexity injunction; Penn Gazette article on digital twins; discussion of agentic AI and platform governance.
9. Student presentations I: selected problems in data privacy and AI; problem definition, affected stakeholders and current legal landscape.				2			**2**	**5**	Group presentation preparation; use AI tools for research, structuring and critique.
10. Student presentations II: data-driven business, policy or legal solutions; critique and peer feedback.				2			**2**	**5**	Group presentation preparation; refine solution/recommendation.
11. Student presentations III: AI, sensitive data, health/wellness data, IoT, surveillance, social media, personalization or related topics.				2			**2**	**5**	Reading and preparation based on selected student topics.
12. Student presentations IV: agentic AI, scraping, platform automation, portability, AI twins, synthetic identities or related topics.				2			**2**	**5**	Reading and preparation based on selected student topics.
13. Student presentations V: legal, technological and ethical evaluation; proposed safeguards, design choices or policy interventions.				2			**2**	**5**	Reading and preparation based on selected student topics.
14. Student presentations VI: final presentation session; synthesis of course themes; transition from presentation work to take-home exam.				2			**2**	**5**	Preparation for presentation delivery; peer feedback; exam preparation.
15. Take-home exam assignment briefing and consultation: issue spotting, structure, expectations and responsible use of AI tools.		2					**2**	**12**	Take-home exam assignment; independent research and writing.
16. Post-exam feedback session: collective feedback, discussion of common issues, reflection on AI-assisted learning and human-centric privacy futures.				2			**2**	**4**	Review feedback and reflect on learning outcomes.
Total:	**16**	**2**		**14**			**32**	**101**	

Assessment strategy	Weight %	Assessment period	Assessment criteria
Take-home examination	60	At the end of the course	Maximum: 6 points. The take-home examination in writing contains 2-3 equally weighted practical assignments which reflect the topics discussed in Lectures 1-8, the student presentations and assigned materials. Students identify legal issues, apply relevant rules and principles, compare enterprise-centric and human-centric approaches, and analyse how data protection and privacy concepts operate in the age of agentic AI. AI tools are encouraged to be used as learning and drafting aids; students remain responsible for verification, documentation, originality and final legal analysis.
Student presentations during practical sessions	30	Practical sessions 9-14	Maximum: 3 points. Students work in groups, normally of two or three, and present a selected data privacy and AI problem. Presentations should define the problem, identify affected stakeholders, explain the legal landscape, analyse legal and technological dimensions, and propose a practical solution, policy recommendation, guideline, business idea or design intervention. Assessment considers issue identification, creativity, legal and technical analysis, responsible use of AI tools, clarity, teamwork and ability to respond to questions.

Preparation and discussions during lectures and practical sessions	10	During semester	Maximum: 1 point. Students prepare by reading assigned materials, watching assigned videos, experimenting with AI tools, comparing outputs where assigned, and actively participating in class discussions. Participation includes constructive engagement with peer presentations and thoughtful reflections on the human-centric perspective. Attendance at all practical sessions is mandatory for every student, irrespective of whether the student is scheduled to present during a particular practical session. If a student misses more than 3 of the practical sessions, he/she must make up the missed practical sessions in accordance with the requirements established by the lecturer; otherwise, participation in the examination is forbidden. The form of make-up work will depend on the topic of the practical session missed.

Author	Year of publication	Title	Issue of a periodical or volume of a publication	Publishing place and house or web link
Compulsory materials				
AMODEI, D.	2026	Interview with Anthropic CEO Dario Amodei	Video interview	https://www.youtube.com/watch?v=MPTNHrq_4LU&t=675s
ARTICLE 29 WORKING PARTY (EUROPEAN DATA PROTECTION BOARD)	1997-2019	Opinions and recommendations		Data base of Article 29 Working Party http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm Database of EDPB: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
ARTICLE 29 WORKING PARTY / EDPB	2017	Guidelines on the Right to Data Portability	Guidelines	EDPB / Article 29 Working Party materials
BYGRAVE, L. A.	2014	Data Privacy Law: an International Perspective		Oxford University Press
HOFFMAN, R.	2024	Reid Hoffman meets his AI twin	Video	https://www.youtube.com/watch?v=rgD2gmwCS10
JURCYS, P., et al.	2025	Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow	Vanderbilt J. of Entertainment & Tech. Law (2025)	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4475106
JURCYS, P., et al.	2025	Who Owns My AI Twin? Lights and Shadows of Data Ownership in a New World of Simulated Identities	SSRN	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4940663
JURCYS, P., et al.	2025	"Private-By-Default": A Principle & Framework for Designing a New World of Personal AI	SSRN	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4839183
JURCYS, P., et al.	2025	Voice Cloning in an Age of Generative AI: Mapping the Limits of the Law & Principles for a New Social Contract with Technology	SSRN	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4850866
JURCYS, P., et al.	2023	Building a 'Green Data' Future: How a Human-Centric Approach to Data and Nudges Can Help Fight Climate Change	2023	https://academic.oup.com/jiplp/article/18/5/386/7113717
JURCYS, P., et al.	2022	The future of international data transfers: managing	The Computer Law & Security	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4010356

		legal risk with a 'user-held' data model	Review, Vol. 46 (2022)	
JURCYS, P., et al.	2020	My Data, My Terms: A Proposal for Personal Data Use Licenses [electronic resource]	Harvard J. of Law & Tech. Digest	jolt.law.harvard.edu/digest/my-data-my-terms
JURCYS, P., et at.	2020	Personal Data Ownership		https://drive.google.com/file/d/15wWFkdpO10HFMoMPVNPY3eK3lc1HeZl8/edit
LEENES, R., BRAKEL R., GUTWIRTH S., HERT P. D.	2017	Data Protection and Privacy: The Age Of Intelligent Machines		Hart Publishing
LEMLEY, M.	2025	The Mirage of Artificial Intelligence Terms of Use Restrictions	SSRN	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5049562
LEMLEY, M.	2024	How Generative AI Turns Copyright Upside Down	SSRN	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4517702
LEMLEY, M.	2022	The Benefit of the Bargain	Stanford Law & Economics Olin Working Paper No. 575	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4184946
MAI, J-E.	2020	Situating Personal Information: Privacy in the Algorithmic Age, in Jorgensen, Human Rights in the Age of Platforms		The MIT Press, shorturl.at/mwT23
PISTOR, K.	2020	Rule By Data: End of Markets?	Law & Contemporary Problems, Vol. 83, pp. 101-124	https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4953&context=lcp
POSNER,	1978	An Economic Theory of Privacy	Regulation, May/June 1978, pp. 19-26	https://www.cato.org/sites/cato.org/files/serials/files/regulation/1978/5/v2n3-4.pdf
PROSSER, W. L.	1960	Privacy	California Law Review	https://lawcat.berkeley.edu/record/1109651?ln=en&v=pdf
JENNIFER ROTHMAN	2025	Who Will Own Your Digital Twin?	The Pennsylvania Gazette	https://thepenngazette.com/who-will-own-your-digital-twin/
SOLOVE, D.	2025	The Great Scrape: The Clash Between Scraping and Privacy	113 California Law Review (forthcoming 2025)	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884485
SOLOVE, D.	2025	Artificial Intelligence and Privacy	77 Florida Law Review 1 (2025)	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111
SOLOVE, D.	2024	Murky Consent: An Approach to the Fictions of Consent in Privacy Law	104 Boston University Law Review 593 (2024)	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743
SOLOVE, D., HARTZOG, W.	2024	Kafka in the Age of AI and the Futility of Privacy as Control	104 Boston University Law Review 1021 (2024)	https://scholarship.law.bu.edu/faculty_scholarship/3820/
SOLOVE, D.	2006	A Taxonomy of Privacy	University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477	
SUNSTEIN, C.	2020	How Much Is Data Privacy Worth?	Journal of Consumer Policy, Vol. 42, pp. 425-224	https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413277
TENE, O.	2011	Privacy: The New Generations. *International*		http://idpl.oxfordjournals.org/content/1/1/15.full.pdf+html

		Data Privacy Law [electronic resource]		
WARREN, S. D.; BRANDEIS, L. D.	1890	Right to Privacy.	Harvard Law Review	groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
Recommended reading				
AARANSON, S., LEBLOND, P.	2018	Another Digital Divide: The Rise of Data Realms and its Implications for the WTO [electronic resource]	Journal of International Economic Law, 21, pp. 245–272	
CH. KUNER, L. A. BYGRAVE, AND CH. DOCKSEY	2019	Commentary on the EU General Data Protection Regulation		Oxford University Press
AMER, K.; NOUJAIM, J. (directors)	2019	The Great Hack	Documentary film	Netflix
BEAUVISAGE, T., MELLET, K.	2020	"Datassets: Assetizing and Marketizing Personal Data" in BIRCH/MUNIESA, Assetization: Turning Things into Assets in Technoscientific Capitalism		The MIT Press, https://bit.ly/31wlzz3
FINCK, M.	2018	Blockchains and Data Protection in the European Union. *European Data Protection Law Review* [electronic resource]		edpl.lexxion.eu/article/edpl/2018/1/6
KUNER, C.	2007	European Data Protection Law: Corporate Compliance and Regulation		Oxford University Press
KUNER, C., et al.	2011	Privacy: an Elusive Concept. *International Data Privacy Law* [electronic resource]		http://idpl.oxfordjournals.org/content/1/3/141.full.pdf+html
KIRBY, M.	2011	The History, Achievement and Future of the 1980 OECD Guidelines on Privacy. *International Data Privacy Law* [electronic resource]		http://idpl.oxfordjournals.org/content/1/1/6.full.pdf+html
LEV-ARETZ, A., STRANDBURG, K.J.	2020	Privacy Regulation and Innovation Policy [electronic resource]	22 Yale J.L. & Tech. 256	https://yjolt.org/sites/default/files/22_yale_j.l._tech._256_2020_privacy-regulation-and-innovation-policy.pdf
MESKYS, et al.	2020	Regulating deep fakes: legal and ethical considerations	Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, pp. 24–31	
MITCHELL, A. and MISHRA, N.	2019	Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute [electronic resource]	Journal of International Economic Law, 22, pp. 389–416	https://academic.oup.com/jiel/article/22/3/389/5521020
MATTTOO, A.; MELTZER, J. P.	2018	International Data Flows and Privacy: The Conflict and Its Resolution	Journal of International Economic Law, 21, pp. 769–789	https://academic.oup.com/jiel/article/21/4/769/5227421
SOLOVE, D.	2008	Understanding Privacy		Harvard University Press
VELIZ, C.	2024	The Ethics of Privacy and Surveillance		OUP

WILL.I.AM.	2019	We need to own our data as a human right—and be compensated for it		https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it