Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

[Find another programme](#)

Compulsory courses

Priv, cybersec & datamanag comp Year 1

Faculty of Law

Orientation Course: Introduction to European Union Law

Full course description

The aim of this introduction course is to create a level playing field among the students enrolled in the Advanced Master in Privacy, Cybersecurity and Data Management with regard to their knowledge in of European Union law linking it to a broader legal context of the Advanced Master set up. This will allow all students to start the program on the same basis with a comparable knowledge. The course may be taken by both students who do not have a legal background and those who have knowledge in law but who would like to refresh or deepen their knowledge in EU law.
The course aims to introduce the working methods of the Advanced Master and to prepare students with the basic knowledge, legal texts and of how to identify, find, read and analyze EU based those legal texts in order to prepare them for the legal courses that follow in the Advanced Master's program. In addition, students will be provided with a general overview of the functioning of the main EU institutions and the legislative process on EU level and the basic information on the relationship between the European legal order and that of EU's Member States. Furthermore, the Court of Justice of the European Union and its jurisprudence will be one important element that will be covered in this course.
Finally, this introductory course is designed as a stepping-stone aims to establish a link toenabling students to enjoy the first course in the Advanced Master's program, European Privacy and Data Protection Fundamentals.

Teaching Method

- Asynchronous, Mix of video, audio text

Assessment Method

- Multiple choice quizzes after each Module on Canvas & One written note on procedural differences in three CJEU judgments

LAW5070
Period 1
1 Sep 2021
22 Oct 2021
[Print course description](#)
ECTS credits:
3.0
Instruction language:
English
Coordinators:

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

- [K.I. Podstawa](#)
- H.R. Kranenborg

Teaching methods:
Coaching
Assessment methods:
Assignment
Faculty of Law

Orientation Course: Introduction to Computer Science and New Technologies

Full course description

The primary aim of the course is to provide an introduction to the fundamental concepts found throughout the field of Computer Science. As such, it is intended as a course on which other courses in the curriculum will build upon. This course is meant to prepare students to address and understand technology-informed legal arguments and form and understand technology-informed opinions. Topics touched upon in this course will further be addressed in the curriculum or form the basis to understand the content of more advanced courses.

Computers are everywhere, and applications (and implications) of Computer Science are very broad and diverse. Therefore, it is important to have a definition of Computer Science in mind, and to understand from a practical point of view why this scientific field is so studied. In this respect, Computer Science is the study of algorithms on formal, hardware, linguistic, and application levels. This definition says that it is the task of the computer scientist to design and develop algorithms to solve a range of important problems in the field of science and engineering, and also in other fields like commerce, psychology, medicine, art and music.

As an overview of the discipline of Computer Science, the course covers a breadth of topics including algorithmic foundations of Computer Science, hardware issues such as number systems and computer architectures, and software issues such as operating systems and networks. Information security topics are also covered, and selected applications of Computer Science are explored, such Artificial Intelligence and Data Science.

Teaching method

- Lectures and PBL-style labs

Assessment method

- A final individual project consisting on a 10 minutes video clip in which each students explains and provides consideration on a popular science article, which they need to select from a suggested pool. This component counts for 60% of the final grade.
- A multiple choice question exam on topics covered in the course. This component counts for 40% of the final grade.

LAW5071
Period 1
1 Sep 2021
22 Oct 2021

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

ECTS credits:
3.0
Instruction language:
English
Coordinators:

- [C.F. Sironi](#)
- [K.I. Podstawa](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment
Faculty of Law

European Privacy and Data Protect Fund

Full course description

Privacy and the protection of personal data have become increasingly relevant over the past decennia. The continuous global development of the information society, which goes hand in hand with an exponential growth of exchange of information, calls for means to control such data flows and to protect individuals whose data it concerns. This is where privacy and data protection kick in. Within the European Union, the rights to privacy and data protection can be found in the EU Charter of Fundamental Rights and in the Treaty on the Functioning of the European Union. At this fundamental level, there is a close relationship with the European Convention on Human Right. The rights to privacy and data protection have been used by the EU Court of Justice to take a firm stance on the protection of personal data. The Court invalidated several EU instruments for breach of the Charter, the most recent example being the EU-US Privacy Shield Decision of the European Commission.
The awareness of the existence of EU data protection rules has increased dramatically due to the application of the General Data Protection Regulation (GDPR) since May 2018, and in particular due to the new power of the supervisory authorities to issue fines, going up to 4% of the worldwide annual turnover, and the requirement to notify security breaches. Data protection compliance has become a priority for companies, and more and more individuals are aware of the rights they can invoke towards entities processing their personal data. Data protection issues are in the news on a daily basis.
Alongside the GDPR, the EU has several other secondary law instruments in place that set out rules on the protection of personal data. These are the ePrivacy Directive for the telecommunications sector, the Law Enforcement Directive and the Data Protection Regulation for EU Institutions and bodies.
The body of case law of the EU Court of Justice in which it has explained these secondary EU rules on data protection has grown steadily over the years.

Assessments

Ø Mid-term written assignment: written note of 1.500 words analyzing a new preliminary ruling
Ø Final exam: open book exam of three hours
- Two general questions concerning the content of the course
- One case study with four sub questions

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

LAW5072
Period 1
1 Sep 2021
22 Oct 2021
[Print course description](#)
ECTS credits:
6.0
Instruction language:
English
Coordinators:

- H.R. Kranenborg
- [K.I. Podstawa](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Written exam
Faculty of Law

EU and Global Cybersecurity Fundamentals

Full course description

This course offers an introduction and up-to-date overview of developments in legal and technical issues relating to cybersecurity. The concept of cybersecurity is elaborated upon, thereby introducing and cryptographic tools and computer-related assets that users and system managers wish to preserve and protect. Various threats and attacks are addressed, laying out the basics of a cybersecurity strategy.

Assessment

MCQ & oral exam
An analysis of the cybersecurity legal framework will be presented, thus introducing the EU cybersecurity strategy, focusing on the
(i) NIS Directive, also touching on the NIS2 Directive proposal;
(ii) the role of ENISA;
(iii) the Cybersecurity Act, including the EU cybersecurity certification framework.
Moreover, the topics of user authentication, access control, database, data center and network security will be touched upon, thereby reviewing different types of authentication methods (e.g., single-factor, multi-factor) and the typical security issues related to authentication and access control. Moreover, malicious software and denial-of-service attacks will be examined, as well as the wide-spectrum of malware threats and countermeasures. The topic of intrusion detection, firewalls, intrusion prevention systems and threat intelligence will be discussed and a cybersecurity-centric reading of the GDPR will be subsequently offered. A broader, general overview toappreciate the multi-dimensionality of cybersecurity will be presented in order to merge the technical and the legal dimension. This course will solidify students' knowledge on computer security technology and its principles, the most relevant EU cybersecurity legal sources, the interconnection with personal data protection and the inner multi- dimensionality of cybersecurity, including its ethical aspects, and its geo-political and economic implication on global scale

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

LAW5073
Period 2
25 Oct 2021
17 Dec 2021
[Print course description](#)
ECTS credits:
6.0
Instruction language:
English
Coordinators:

- [M.H.M. Winands](#)
- [K.I. Podstawa](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment
Faculty of Law

Data Protection Compliance Management, Leadership and Communication

Full course description

This course integrates the academic knowledge gained in the first courses of the master programme and trains students to translate their knowledge to the business practice. From this perspective, it deepens the students' acquired skills and therefore complements those core courses. In particular, it requires the students to learn effective interdisciplinary communication and leadership skills, while also requiring them to learn about certain theoretical concepts.
The focus of this course is placed on the students' ability to critically reflect on and apply methodologies of broadly understood data breach management skills.
Hence, creating a solid data protection compliance framework in an organisation is not simply about specific competences on the subject matter. Leadership and communication skills are necessary for the correct management of relevant technical and organisational processes. Therefore, the course provides participants with extended training on the skills necessary to ensure compliance with personal data protection rules through building up a resource-efficient data protection-compliant management framework.

LAW5074
Period 3
3 Jan 2022
28 Jan 2022
[Print course description](#)
ECTS credits:
1.5
Instruction language:
English
Coordinators:

- [K.I. Podstawa](#)

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

- L.E. Kuusniemi

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Participation
Faculty of Law

Advanced Cybersecurity and Global Cybersecurity Strategy

Full course description

The course builds upon the knowledge acquired in the course 'EU and Global cybersecurity fundamentals'. It expands on the previous knowledge of the students and addresses advanced concepts of cybersecurity, including risk assessment and management, regulatory compliance and compliance management. Specifically, it focuses on Global Approval and Compliance for devices and operations, including (i) European Cyber certification and compliance: EU requirements, Cyber Security certification, CE approval, etc. (ii) US Cyber certification and compliance: NIST, FCC, PCI DSS 2.0, Cloud Act, etc. (iii) as well as Chinese and Indian certifications and standards in the field. Lastly, it ties all of this together by introducing a global strategy dimension; here, students will learn how to align cybersecurity with business strategy and IT strategy.

LAW5077
Period 5
11 Apr 2022
10 Jun 2022
Print course description
ECTS credits:
6.0
Instruction language:
English
Coordinators:

- M.H.M. Winands
- K.I. Podstawa

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment
Faculty of Law

Compr Risk Assessm Data Prot Imp Ass

Full course description

This course aims at providing a solid and practice-oriented methodology to carry out the necessary risk assessment on all envisaged data processing activities, in order to identify those processing operations that are likely to result in a high risk for data subjects and consequently obliges controllers to perform a full Data Protection Impact Assessment (DPIA).

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

Such exercise is an essential tool to design data processing operations that are both legally compliant and ethically respectful of the rights and freedoms of data subjects. Therefore, in this skills course the students will be provided with efficient ways to plan and conduct systematic risk assessment activities and to carry out specific DPIAs, where needed. Different models and approaches of risk assessments and methodologies to perform a DPIA will be explained, critically discussed and applied in practice. (In addition, the course will deal with risk assessments that are to be carried out before processing may take place and be closely linked to risk assessments that need to be carried out once processing took place, for instance after the occurrence of personal data breaches.)

The students will be required to prepare their own risk assessment plan along the approaches proposed and to conduct DPIAs on the basis of two practical case studies that will be provided prior to the start of the course. One additional full DPIA will be conducted as group exercise in form of a case study given during the course. After completing the course, the students will have the capacity to build a robust data protection compliance framework pursuant to the risk-based approach and to the principles of Data Protection by Design and Data Protection by Default.

Assessments:

- Group assignment
- Individual assignment

LAW5075
Period 3
3 Jan 2022
28 Jan 2022
[Print course description](#)
ECTS credits:
1.5
Coordinators:

- P. Balboni
- [K.I. Podstawa](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assessment, Presentation
Faculty of Law

Advanced (International) Privacy and Data Protection

Full course description

Advanced (International) Privacy and Data Protection is the second data protection related course of the Advanced Master's programme in Privacy, Cybersecurity and Data Management. In this course, students will build upon their knowledge acquired in the first course 'EU Privacy and Data Protection Fundamentals' to apply the underlying principles and basic features of the EU data protection regime to other data protection rules around the world in a comparative manner. For instance, it covers the transfer of personal data to third countries and international organizations from different angles. In addition, students will be acquainted with different fields governed by legislation that requires the processing of personal data. Students will learn to assess how such

legislative measures may have an impact on the right to privacy and data protection and activities undertaken by a variety of actors involved in the process.

The course builds upon the knowledge acquired in the course 'EU Privacy and Data Protection Fundamentals' by addressing pressing privacy and data protection questions more in depth and by focusing on issues of global relevance, pertinent for multinational companies and international organisations. The fundamental international data protection principles (i.e. Transparency, Data Minimisation, Purpose Limitation, Security, Data Quality, Access and Correction, Accountability) will be explained also making reference to their application in jurisdictions outside the European Union, including International Organisations.

International instruments such as the EU-US Umbrella Agreement, Binding Corporate Rules, Agreements on Passenger Name Records (PNR) and the Terrorist Finance Tracking Programme (TFTP) are put forward for a detailed discussion. In addition, Advanced (International) Privacy and Data Protection covers trends on the adoption of rules that seek to make it easier for police and judicial authorities to access electronic evidence held by private companies. Finally, the course addresses the essential data protection risks related to automated individual decision making and profiling as well as other challenges that emerge with regard to technological developments and the protection of personal data.

Assessments:

- Participation to tutorial discussions
- Mid-term assignment (optional): written note of 1.500 words comparing EU and third country data protection legislation.
- Additional assignment (optional): creating a mind map describing the process of international transfers under the GDPR
- Final Exam: open book exam of three hours
  - Two general questions concerning the content of the course and one case study

LAW5076
Period 4
1 Feb 2022
1 Apr 2022
Print course description
ECTS credits:
6.0
Instruction language:
English
Coordinators:

- K.I. Podstawa
- H.R. Kranenborg

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Written exam, Attendance

Advanced Master in Privacy, Cybersecurity and Datamanagement Year II compulsory courses

Faculty of Law

Digital Trust: ePrivacy and the Protection of Personal Data in Electronic Communications

Full course description

The course familiarises the students with a highly topical issue of e-Privacy by discussing in details questions related to the e-Privacy Directive and its potential legislative successor, e-Privacy Regulation. The ePrivacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. It also guarantees the free movement of electronic communications data, equipment and services in the EU. The European legislation is keeping up with the fast space at which IT-based services are developing and evolving by proposing a e-Privacy Regulation. The students will explore the current challenges related to the interaction between data protection rules and eprivacy realities - in particular from the perspective of the intersection of commonly used IT tools (as Google analytics) and their impact on fundamental rights. They will explore, in particular the context of online advertising as the one of the most problematic business environments from this perspective. Importantly, the course will take place mostly in the synchronous face-to-face manner to maximise the peer-to-peer learning.

LAW5079
Period 1
1 Sep 2021
22 Oct 2021
Print course description
ECTS credits:
3.0
Coordinator:

- K.I. Podstawa

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Final paper
Faculty of Law

Cybersecurity Governance and Management

Full course description

This course focuses on the practices and processes of cybersecurity management and governance and provides the students with practical guidance on what the management of cybersecurity involves. It further offers an overview of Information Security Management Systems, focusing on what an information security management system is and why it is so important in developing a security plan for protecting systems and data. In this context, standards such as the ISMS frameworks such as ISO 27001, COBIT, NIST 800 will be addressed. Next to this, the element of risk management is elaborated on and put in context by addressing what cybersecurity risk management is and by giving an overview of what risk management is about, how to manage risk, why risk management is important. Here, an overview of the different risk management frameworks, ISO

27005, Octave, FAIR, etc. will be provided. Lastly, the concepts of security metrics and security key performance indicators will be introduced.

LAW5080
Period 1
1 Sep 2021
22 Oct 2021
[Print course description](#)
ECTS credits:
3.0
Coordinator:

- [M.H.M. Winands](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assessment, Written exam
Faculty of Law

Leadership Development Trajectory

Full course description

This course is set up to develop students' leadership effectiveness in a personalized and engaging way. An important characteristic of the trajectory is that it stimulates learning which students can directly apply to current leadership challenges. These can be challenges related to personal leadership (leading oneself) or leadership of others with or without formal authority. The course is designed to empower students to discover how they can effectively lead in the field of data protection and cybersecurity and deal with new regulation and on-going developments in the privacy and cybersecurity market. Either from a leadership position in a hierarchy, or from taking on a leadership role in something that matters to them. Developing leadership is first and foremost a personal learning trajectory characterized by building self. The design of this leadership development course is built on the assumption that students take personal ownership of their trajectory. This means that students are in the driver's seat when it comes developing their own leadership trajectory.

Assessments:

- Intake questionnaire
- training sessions
- individual meetings

LAW5081
Period 2
25 Oct 2021
17 Dec 2021
[Print course description](#)
ECTS credits:
3.0
Coordinator:

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

- [M.G. Heijltjes](#)

Teaching methods:
Project-Centered Learning
Assessment methods:
Assignment
Faculty of Law

ICT and Data-related contracts

Full course description

We live in the "Big Data Era", which is characterised by the so called "Data gold rush". This means that large amounts of different types of data are produced from multiple sources and exchanged between several parties on a daily basis at high speed requiring increasingly powerful processors and algorithms to process and to effectively analyse them. Not all of this information is personal, but businesses and governments are more and more using big data to understand, predict and shape human behaviour. Big data is therefore putting strain on not only privacy and data protection, but other fundamental rights including freedom of expression and non-discrimination. Contracts are becoming increasingly relevant to regulate business models based on data and also to allocate privacy roles (e.g. controllerprocessor, joint-controllership) and the relevant compliance duties and obligations. This course will familiarise the students with the technology deployed and typical business models based on data analysis and data sharing of ICT services. We will discuss phenomena like cloud computing, big data,
149 analytics, internet of things, online behavioural advertising, programmatic advertising, data management platform etc. Moreover, students will learn how ICT and data related contracts are typically structured. During the course, legal issues and solutions concerning privacy, data security, contractual, consumer protection and intellectual property matters will also be discussed providing a multidisciplinary approach to the subject matter.

Assessments:

10% Participation during the course;
30% Practical assignments (in the forms of group presentations and group written assignments) and feedback to assignments of teachers and peers;
60% Final written exam (i.e. drafting of an ICT/data-related contract)

LAW5082
Period 2
25 Oct 2021
17 Dec 2021
[Print course description](#)
ECTS credits:
3.0
Coordinator:

- P. Balboni

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Participation, Written exam

Data Protection and Security Assessment/Audit: Case Study of Cloud Computing

Full course description

The course deepens the legal-theoretical background, the methodologies and the standards for privacy, data protection and cybersecurity assessments/audit activities, contextualizing and explaining
their usefulness for specific cases. Cloud computing will be used as complex scenario to practise the relevant assessment/audit skills. The course explains different cloud models, privacy and regulatory issues to consider with cloud computing, how to risk assess the cloud with respect to the protection of personal data, the managing of security threads in the cloud, the selections of cloud vendor based on the "privacy levels" that they offer. More precisely, the students are also introduced to principles and practice of cybersecurity auditing in cloud environments through auditing frameworks, standards
and technical measures, including vulnerability testing and penetration testing. The course finishes with a hands-on exercise in which students conduct a mock personal data protection on security audit
on a service provided by a cloud service provider.

Assessments:

30% Participation during the course;
30% Practical assignments (in the forms of group presentations and group written assignments) and feedback to assignments of teachers and peers;
60% Final written exam

LAW5083
Period 3
3 Jan 2022
28 Jan 2022
Print course description
ECTS credits:
3.0
Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Participation, Written exam
Faculty of Law

Ethics, Accountability and Corporate Social Responsibility in the Digital Age

Full course description

Scandals surrounding the misuse of data are mounting casting doubt on the current approach

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

towards how we use data and putting into question not only European but the global set up of privacy rules. An accountable and sustainable approach regarding the use of (personal) data as well as the integrity and security of the processing of data is required to ensure that the tension between, on the one hand, the protection of individuals' fundamental rights – such as the protection of personal data – and, on the other hand, data usage practices for value creation, reflect the societal needs and expectations. The regulators (within EU, European Data Protection Supervisor and the European Commission) are increasingly and consistently stimulating an ethical approach to privacy and personal data protection, in part in addition to existing GDPR rules, but in part in their lieu, especially in the global setting. The course aims to translate such recommendations into practical applications. It covers questions of legal accountability, social responsibility and related ethical compliance that go beyond the strict privacy and data protection legislative regulation.
issues. More precisely, increased processing of vast amounts of personal data, also in the context of business intelligence, imposes on companies and on organisation in general additional social and ethical responsibility, as data processing should not lead to abuses or manipulation of individuals/data subjects.

Assessments:

- 70% final paper;
- 20% written assignments, discussed in tutorials;
- 10% Peer Review

LAW5084
Period 4
1 Feb 2022
1 Apr 2022
[Print course description](#)
ECTS credits:
3.0
Coordinator:

- [K.I. Podstawa](#)

Teaching methods:
Lecture(s), PBL
Assessment methods:
Assignment, Final paper
Faculty of Law

The Future of Privacy, Cybersecurity and

Full course description

The course 'The Future of Privacy, Cybersecurity and Data Management: New technologies and new approaches' is the last module of the programme and it is a forward-looking course that touches upon future, potential and unresolved open questions related to the fields of privacy, cybersecurity and data management. The course ties together all previous subjects in an interdisciplinary way and requires students to work in teams to solve forward-looking and interdisciplinary challenges at the forefront of privacy, cybersecurity and data management. During the course, student teams will work on one of a number of challenges presented by challenge owners. Challenge owners will be actors from industry, regulators or civil society who will present a specific challenge regarding the

future of privacy, cybersecurity and/or data management. During the course, students will be exposed to challenge owners and industry thought leaders through a series of workshops and online webinars to discuss emerging trends and practices at the forefront of privacy, cybersecurity and data management. The student teams are tasked with solving these issues and will present their solution in a final conference 150 and submit their solution (paper/prototype/etc.) for assessment to the challenge owner and the course staff.

Assessments:

- 20% Hackathon presentation (each team member must present);
- 20% solution to the Hackathon challenge (paper/prototype/etc.);
- 10% peer assessment of the solution;
- 50% Reflection paper

LAW5085
Period 4
1 Feb 2022
1 Apr 2022
[Print course description](#)
ECTS credits:
3.0
Coordinator:

- [M. Brkan](#)

Teaching methods:
Lecture(s), PBL, Presentations
Assessment methods:
Assessment, Assignment, Presentation
Thesis

Advanced Master in Privacy, Cybersecurity and Data Management, Master Thesis Year I

Faculty of Law

Master Thesis Year 1 Adv master Priv Cyb

Full course description

Master's Thesis procedure involves two separate components that need to be followed by students. The process begins with Master's Thesis I component during Period 5 and Period 6 of the first academic year of the course. In order to equip candidates with the knowledge to independently formulate a research question, conduct research and write a thesis, a seminar on thesis writing and research methods will be held at the end of the first academic year in July. In this series of seminars and workshops, candidates will be acquainted with various research methods and approaches, including conducting literature reviews, defining a research question, finding an appropriate methodology and thesis writing and legal English workshops. In the course of seminars students will be encouraged to engage critically with sources and with themes of their enquiry. Subsequently,

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

students will present their research proposal in the course or thesis writing seminar. Subsequently, they will develop their thesis following the guidance of the assigned superviser.

LAW5078
Period 6
6 Jun 2022
1 Jul 2022
[Print course description](#)
ECTS credits:
3.0
Coordinators:

- [M. Brkan](#)
- [K.I. Podstawa](#)

Advanced Master in Privacy, Cybersecurity and Data Management, Master Thesis Year II

Faculty of Law

Advanced Master in Privacy, Cybersecurity and Data Management, Master Thesis Year II

Full course description

During the second academic year, in the course of Master's Thesis II component students choose their thesis topic with the help of staff members. The topics shall be closely related to the specific subject matter of the programme. In order to ensure that candidates are on track with their thesis and are able to finalize the programme in a timely manner, a number of stepping stone events are planned during the second year: Candidates will work together with a supervisor to draft and submit a thesis outline. During the second Period of the second year, candidates will present their outline. This will be the first instance
of the written exchange between the student and the supervisor. Students will work on the thesis to draft the first version that will need to be presented to the supervisor in June of the second academic year. After the exchange of feedback, students will submit the final version of the thesis by 31 August of the second academic year.
In the course of the supervision relationship, supervisors and students are at liberty to define the milestones of the process and contact moments, save for the obligation imposed on supervisors to provide written feedback twice in the process of writing (in reaction to the submitted outline and first draft of the thesis).

LAW5086
Period 5
11 Apr 2022
10 Jun 2022
[Print course description](#)
ECTS credits:
9.0
Coordinator:

Advanced Master in Privacy, Cybersecurity, Data Management and Leadership

- [M. Brkan](#)