

Orientation Course: Introduction to European Union Law

Faculty of Law

LAW5070

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

K.I. Podstawa

Teaching methods:

Coaching

Assessment methods:

Written exam, Assignment

Full course description

The aim of the course is to ensure the common minimal standard of knowledge in the area of EU law to all students participating in the Programme. The course will be offered in an asynchronous manner; however, additional support may be offered by the Faculty through Q&A sessions and feedback sessions by the staff of the Programme. The course is developed with the view of supporting students in passing the final exam of the course corresponding in terms of the body of knowledge to the European Union Law entrance exam, customarily used at the beginning of Master's courses offered by the University of Maastricht Faculty of Law.

Assessment

- MCQ and case study

Teaching Method

- Asynchronous, Mix of video, audio text

Orientation Course: Introduction to Computer Science and New Technologies

Faculty of Law

LAW5071

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

T. Fabry

Teaching methods:

PBL

Assessment methods:

Assignment

Keywords:

IT concepts, cybersecurity concepts, technology

Full course description

Introduction to Computer Science and Technologies is aimed at introducing the fundamental concepts of IT systems, computer science and foundational cybersecurity. This course serves as the stepping-stone for the other courses on cybersecurity and data protection. During this course, students will learn and become familiar with the principles, concepts and terms relating to IT systems and computer science, and their relevance for cybersecurity. This acquired knowledge will assist students in the following and comprehension of the more advanced cybersecurity and data protection concepts that they will study during the Advanced Master's program.

Course objectives

- Students are trained in the fundamental IT knowledge and skills required to understand cybersecurity.
- Students familiarize with the fundamental cybersecurity "glossary".
- Students demonstrate the ability to confidently start the journey to cybersecurity courses.

Prerequisites

Pre-requisites:

N/A

Recommended prior knowledge:

N/A

Recommended reading

Mandatory reading:

TBD

Recommended reading:

TBD

European Privacy and Data Protection Fundamentals

Faculty of Law

LAW5072

Period 1:

1 Sep 2025

24 Oct 2025

Credits:

6.0

Coordinator:

H.R. Kranenberg

Teaching methods:

PBL

Assessment methods:

Written exam, Assignment

Keywords:

Data protection, EU law

Full course description

This course serves as the basic building block for all other privacy and data protection related courses of the Advanced Masters. It is a prerequisite for the understanding of EU privacy and data protection legislation *within* the EU since it introduces the students to core concepts of privacy and data protection.

These core concepts will be further translated into international settings in the course 'Advanced (International) Privacy & Data Protection', which is a continuation of the present course. The Advanced (International) Privacy & Data Protection course will *inter alia* deal with data protection laws in other regions of the world and legislative endeavours that have an impact on the protection of personal data.

The present course also introduces the students to the core academic approaches in the field of privacy and data protection, which are then given a practical and more detailed implementation during the tutorials. Needless to say, Year 2 of the programme will rely heavily on the knowledge acquired in the course of Foundations and Advanced courses.

Course objectives

EU Privacy and Data Protection Fundamentals is the first course of the Advanced Master's programme in Privacy, Cybersecurity and Data Management. In this course students are introduced to the underlying principles and basic features of the EU data protection regime.

The main objectives of this course are that students:

1. Understand the origins of the current EU data protection framework, which lie in the fundamental right to privacy;
2. Understand how this fundamental rights perspective influences the way in which the EU Court of Justice approaches questions relating to data protection;
3. Become familiar with the different Union laws on data protection, their main features and the relevant case law of the EU Court of Justice.

Prerequisites

Pre-requisites:

Completion of the introductory course to the EU law and/or demonstrated prior knowledge of the EU law foundations..

Recommended prior knowledge:

Prior knowledge of foundational concepts of EU law.

Recommended reading

Mandatory reading:

The Fundamental Rights Agency's Handbook on European Data Protection Law provides an overview of the EU and ECHR applicable legal frameworks and explains the key case law of the CJEU and the ECtHR, see: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.

H.R. Kranenborg, "Commentary on Article 8 of the EU Charter of Fundamental Rights" in S. Peers, T. Hervey, J. Kenner and A. Ward (eds) Commentary on the EU Charter of Fundamental Rights (Hart Publishing, 2021) – the text will be made available on Canvas.

European Court of Justice Research and Documentation Directorate, Fact sheet: Protection of personal data, July 2024. Available here (also in different language versions):

https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf

Recommended reading:

C. Kuner, L. Bygrave, C. Docksey (eds), *The EU General Data Protection Regulation – A Commentary* (OUP, 2020) and its online update of 2021, see

https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf.

Leadership Development Trajectory

Faculty of Law

LAW5081

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

R.J.M. Speijcken

Teaching methods:

Training(s), Project-Centered Learning

Assessment methods:

Assignment

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 to developing their own leadership trajectory.

Cybersecurity Fundamentals

Faculty of Law

LAW5073

Period 2:

27 Oct 2025

19 Dec 2025

Credits:

6.0

Coordinator:

T. FabryP. Balboni

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Written exam, Oral exam

Keywords:

Cybersecurity, Information Security, Data Protection, Cybersecurity Strategies, NIS2, DORA, Cyber Resilience Act, Cyber Security Act, Artificial Intelligence, AI

Full course description

Cybersecurity strategies and laws are rapidly evolving in the EU and around the globe as a result of the growing concerns brought on by digitalisation, the quick uptake of new technology, and the rise in cyberattacks. With the primary purpose of addressing new and advancing technological developments, cybersecurity risks, and actors, many countries around the globe have released their cybersecurity strategies. Coherently, in the last few years, several new EU cybersecurity laws have been established, and some existing laws governing cybersecurity in the EU have been amended to reflect and capture the new emerging and advancing landscape of the cyber world and technology. Additionally, proposals for additional cybersecurity legal instruments are currently under discussion at the EU level, with the intent to increase resilience and sovereignty and develop the necessary skills (i.e., capacity building) in the region.

Staying up to date with the fast-changing landscape of cybersecurity laws and regional strategies is necessary to ensure the digital and cyber well-being of citizens, the effective functioning of governments, and the compliance of businesses.

“*EU and Global Cybersecurity Fundamentals*” is the first course on cybersecurity in the Advanced Master’s Programme. It therefore explores and analyses the European Union cybersecurity strategy as well as those of other countries (e.g., the UK, US, Japan, Brazil, Kenya, and Australia) and a number of the major EU cybersecurity legal frameworks. It covers the EU cybersecurity legislation with the intent of comprehending the security requirements mandated by the law. The course discusses how these laws will affect organisations and, at the same time, provides the best practices, frameworks, and standards that organisations should implement before and after a cybersecurity or data breach incident occurs, thus improving their cybersecurity posture and ensuring compliance with the laws.

Teaching method:

- 7 lectures
- 6 tutorials

Course objectives

- Acquire a ‘dictionary’ to understand the relevant cybersecurity and data protection laws and policies and develop a common language to communicate on cybersecurity
- Learn about existing and future developments and priorities to mitigate the risk associated with cybersecurity at international level.
- Learn the cybersecurity implications of legal instruments like the GDPR
- Analyse, understand and apply EU cybersecurity legislation (NIS2, Cybersecurity Act, DORA, CRA, etc.)
- Learn the cybersecurity implication of the AI Act and how this legal instrument relates to the EU cybersecurity legislative domain

Prerequisites

N / A

Recommended reading

TBD

Advanced Privacy and Data Protection Law

Faculty of Law

LAW5076

Period 4:

2 Feb 2026

2 Apr 2026

Credits:

6.0

Coordinator:

M.S. Magierska

Teaching methods:

PBL

Assessment methods:

Written exam, Assignment

Keywords:

Data protection, EU law, GDPR, privacy

Full course description

This course continues the understanding of core concepts of EU privacy and data protection legislation the students were acquainted with in the European Privacy and Data Protection Fundamentals.

During 'Advanced Privacy and Data Protection', the students will encounter different areas that intersect with data protection rules. In addition, the core concepts introduced in the LAW5072 course will be translated into situations where data protection overlaps with other fields, such as consumer law or competition law, or other concepts (vulnerability) or is examined in various contexts (that of global data protection rules or law enforcement). The students will also analyse, from the perspective of the GDPR, how other global governance regimes regulate privacy and data protection. Moreover, they will be introduced to basic privacy and data protection theories and ideas to help them theoretically orientate their master's thesis in Year 2.

The present course will further substantiate the academic approaches in the privacy and data protection field, which will then materialize in the practical application of the accumulated skills during the tutorials. In addition, the students will be invited to test their writing skills in the context of the bootcamp.

Course objectives

EU Privacy and Data Protection Fundamentals is the first course of the Advanced Master's programme in Privacy, Cybersecurity and Data Management. In this course students are introduced to the underlying principles and basic features of the EU data protection regime.

The main objectives of this course are for the students to be able to:

1. Understand the relationship of EU data protection law at different levels as well as the rules on the protection of personal data in various areas;
2. Get familiar with the general global trends in privacy and data protection governance;
3. Grasp the impact that technological advances and recent developments may entail on the rights to privacy and the protection of personal data;
4. Understand the balancing dynamics that guide the EU's data protection rationale (and, in a broader perspective, the EU's data governance): security vs. fundamental rights, individual rights vs. economic interests, and innovation vs. regulation.

Prerequisites

Pre-requisites:

Completion of the LAW5072.

Recommended prior knowledge:

Prior knowledge of foundations of competition and consumer law.

Recommended reading

Mandatory reading:

The Fundamental Rights Agency's Handbook on European Data Protection Law provides an overview of the EU and ECHR applicable legal frameworks and explains the key case law of the CJEU and the ECtHR, see: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.

H.R. Kranenborg, "Commentary on Article 8 of the EU Charter of Fundamental Rights" in S. Peers, T. Hervey, J. Kenner and A. Ward (eds) Commentary on the EU Charter of Fundamental Rights (Hart Publishing, 2021) – the text will be made available on Canvas.

European Court of Justice Research and Documentation Directorate, Fact sheet: Protection of personal data, July 2024. Available here (also in different language versions):

https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf

Recommended reading:

C. Kuner, L. Bygrave, C. Docksey (eds), The EU General Data Protection Regulation – A Commentary (OUP, 2020) and its online update of 2021, see

https://fdslive.oup.com/www.oup.com/academic/pdf/law/GDPRCommentary_ArticleUpdates.pdf.

Advanced Cybersecurity

Faculty of Law

LAW5077

Period 5:

13 Apr 2026

12 Jun 2026

Credits:

6.0

Coordinator:

T. Fabry

Teaching methods:

PBL

Assessment methods:

Presentation, Assignment, Oral exam

Keywords:

Security, cybersecurity, security technology, privacy technology

Full course description

This course supplements the knowledge acquired in “EU and Global Cybersecurity Fundamentals.” The course builds on the students' prior knowledge, providing the students with additional technical, technological and scientific information about cybersecurity concepts. The course aims to ensure that the students gain an understanding of how to apply technical cybersecurity measures to comply with various cybersecurity and data protection laws, from a technological perspective.

The course has a threefold aim:

- to equip the students with the relevant (high-level understanding of the) technical-scientific aspects of cybersecurity;
- to equip the students with the ability to communicate with cybersecurity experts, software architects, and administrators; and
- to equip the students with the ability to understand academic research in and related to cybersecurity and privacy.

Course objectives

- Students are able to understand academic research in fields related to privacy and cybersecurity law & technology, management and leadership.
- Students are able to combine knowledge from privacy and cybersecurity.

- Students have an in-depth understanding of the novelties in the field of cybersecurity law and technology and relate them to the topical societal challenges in these fields.
- Students demonstrate the ability to communicate with cybersecurity experts, software architectures, and administrators.
- Students work in multicultural teams and environments.

Prerequisites

Prerequisites:

Having followed LAW5073

Recommended prior knowledge:

Basic concepts of IT systems

Recommended reading

TBD

Orientation Course: Introduction to European Union Law

Faculty of Law

LAW5070

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

K.I. Podstawa

Teaching methods:

Coaching

Assessment methods:

Written exam, Assignment

Full course description

The aim of the course is to ensure the common minimal standard of knowledge in the area of EU law to all students participating in the Programme. The course will be offered in an asynchronous manner; however, additional support may be offered by the Faculty through Q&A sessions and feedback sessions by the staff of the Programme. The course is developed with the view of supporting students in passing the final exam of the course corresponding in terms of the body of knowledge to the European Union Law entrance exam, customarily used at the beginning of Master's courses offered by the University of Maastricht Faculty of Law.

Assessment

- MCQ and case study

Teaching Method

- Asynchronous, Mix of video, audio text

Orientation Course: Introduction to Computer Science and New Technologies

Faculty of Law

LAW5071

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

T. Fabry

Teaching methods:

PBL

Assessment methods:

Assignment

Keywords:

IT concepts, cybersecurity concepts, technology

Full course description

Introduction to Computer Science and Technologies is aimed at introducing the fundamental concepts of IT systems, computer science and foundational cybersecurity. This course serves as the stepping-stone for the other courses on cybersecurity and data protection. During this course, students will learn and become familiar with the principles, concepts and terms relating to IT systems and computer science, and their relevance for cybersecurity. This acquired knowledge will assist students in the following and comprehension of the more advanced cybersecurity and data protection concepts that they will study during the Advanced Master's program.

Course objectives

- Students are trained in the fundamental IT knowledge and skills required to understand cybersecurity.
- Students familiarize with the fundamental cybersecurity "glossary".
- Students demonstrate the ability to confidently start the journey to cybersecurity courses.

Prerequisites

Pre-requisites:

N/A

Recommended prior knowledge:

N/A

Recommended reading

Mandatory reading:

TBD

Recommended reading:

TBD

ePrivacy and the Protection of Personal Data in Electronic Communications

Faculty of Law

LAW5079

Period 1:

1 Sep 2025

24 Oct 2025

Credits:

3.0

Coordinator:

C.F. Mondschein

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Assignment, Assessment

Keywords:

privacy, data protection, electronic communication, ePrivacy, rivacy

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 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 familiarise with the main changes that the e-Privacy Regulation aims to introduce in this scenario, e.g., the more user friendly rules on cookies and tracking technologies; new opportunities for telecoms operators (once consent is given for communications data - content and/or metadata - to be processed, traditional telecoms operators will have more opportunities to provide additional services and to develop their businesses, for example, they could produce heat maps indicating the presence of individuals; these could help public authorities and transport companies when developing new infrastructure projects; bans on unsolicited electronic communications by emails, SMS and automated calling machines; etc.

Assessment methods

70% final exam (individual assessment), 30% case study (group assessment)

Cybersecurity Governance and Management Deep-dive

Faculty of Law

LAW5080

Period 1:

1 Sep 2025

24 Oct 2025

Credits:

3.0

Coordinator:

T. Fabry

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Written exam, Assignment, Assessment

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.

Leadership Development Trajectory

Faculty of Law

LAW5081

Year:

1 Sep 2025

31 Aug 2026

Credits:

3.0

Coordinator:

R.J.M. Speijcken

Teaching methods:

Training(s), Project-Centered Learning

Assessment methods:

Assignment

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 to developing their own leadership trajectory.

Data Governance

Faculty of Law

LAW4089

Period 2:

27 Oct 2025

19 Dec 2025

Credits:

6.0

Coordinator:

C. Teleki

Teaching methods:

Assessment methods:

Keywords:

Full course description

Course objectives

Recommended reading

ICT and Data-related contracts

Faculty of Law

LAW5082

Period 3:

5 Jan 2026

30 Jan 2026

Credits:

3.0

Coordinator:

C. TelekiP. Balboni

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Written exam

Keywords:

Data Act, Data-related Contracts, ICT Contracts, Data-driven economy, European Data Strategy, Data processing agreements, Joint controllership agreements

Full course description

Recently the European legislator has enacted the Data Act, which is a comprehensive legislative effort to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data. The Regulation entered into force on 11 January 2024 with direct applicability on 12 September 2025 and it is a key pillar of the European data strategy.

Contracts are, firstly, key in the operationalization of the Data Act in terms of “mandatory” and “voluntary” data sharing and provision of “data processing services” (e.g., ICT and cloud computing services). Secondly, contracts are playing a fundamental role in allocating privacy roles (e.g., controller-processor, joint-controllership) and the relevant data protection compliance duties and obligations.

This course will familiarise the participants with ICT and data-related contracts. How they are typically structured, the main provisions, typical issues, solutions. Moreover, the participants will be familiarized with the work of the Expert Group on B2B data sharing and cloud computing contracts which Paolo Balboni was part of and the Model Contractual Terms and Standard Contractual Clauses.

A number of such agreements will be analysed by carrying out practical exercises aimed at training the participants to recognise - among other features - the existence of the necessary elements, the applicable law and competent jurisdiction both for issues related to the performance of the contract and for the processing of personal data, unfair clauses, non-compliances with the applicable legal framework, inconsistencies, limitations of liability and indemnity clauses, etc.

More precisely, during the course, legal issues and solutions concerning privacy, data security, data sharing, contractual, intellectual property matters will be discussed, providing an interconnected multidisciplinary approach to the subject matter.

Teaching method:

- 3 lectures
- 2 tutorials

Course objectives

Course objectives:

- Analyse and understand data-related legislation, especially how the Data Act interacts with other European legislations (e.g., GDPR, DMA, DSA, etc.)
- Learn about the main topics to be analysed and negotiated regarding B2B ICT service agreements and data-related provisions, including pitfalls and points of interest in each topic from the perspective of the service provider and customer.
- Develop knowledge of the Data Act and, specifically of the provisions related to mandatory and voluntary data sharing and practise it.

Prerequisites

N/A

Recommended reading

TBD

Communication in Data Management

Faculty of Law

LAW5074

Period 4:

2 Feb 2026

2 Apr 2026

Credits:

1.5

Coordinator:

K.I. Podstawa

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Participation, Assignment

Full course description

This course is tailor-made for high-level managers in both multinational companies as well as small and medium-sized enterprises and public organisations. It provides the students with extended training on skills necessary to ensure compliance with personal data protection rules through building up of a resource-efficient data protection-compliant management framework. A sound methodology to assure that the fundamental principles on privacy and data protection are complied with and integrated in the design of the relevant data processing activities (pursuant to the core principles of Data Protection by Design and Data Protection by Default) will be provided. Necessary skills for organising adequate training to staff, assertiveness competencies to ensure budget for compliance programmes, sharp ability of information collection and privacy tool sourcing, as well as skills of interdisciplinary communication will be intensively trained. Finally, a case study on preventing and responding to data breaches will be used to concretely apply the notions learned during this course.

Integrated Risk Assessment

Faculty of Law

LAW5075

Period 4:

2 Feb 2026

2 Apr 2026

Credits:

1.5

Coordinator:

P. Balboni K.I. Podstawa

Teaching methods:

PBL, Lecture(s)

Assessment methods:

Presentation, Assessment

The Future of Privacy, Cybersecurity and Data Management

Faculty of Law

LAW5085

Period 5:

13 Apr 2026

12 Jun 2026

Credits:

3.0

Coordinator:

C. Teleki

Teaching methods:

PBL, Lecture(s), Presentation(s)

Assessment methods:

Presentation, Assignment, Assessment

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.

Academic and Thesis Writing Bootcamp (Master's Thesis I)

Faculty of Law

LAW5078

Period 3:

5 Jan 2026

30 Jan 2026

Credits:

3.0

Coordinator:

K.I. Podstawa

Teaching methods:

Assessment methods:

Master Thesis II

Faculty of Law

LAW5086

Year:

1 Sep 2025

31 Aug 2026

Credits:

9.0

Coordinator:

K.I. Podstawa

Teaching methods:

Assessment methods:

Full course description

During the second academic year, in the course of Master's Thesis II component students choose their thesis topic, if necessary, 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).

