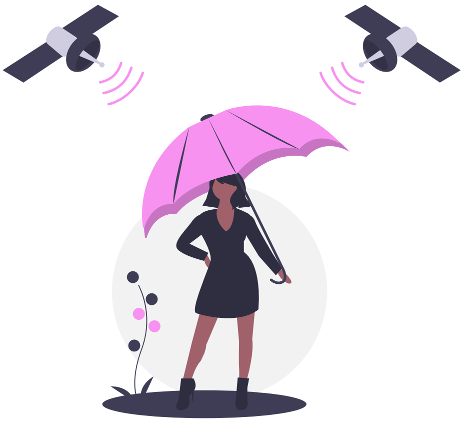
Big Data, Human Rights, and Human Security Syllabus



Contents

Who coordinates this course?

Sarah Eskens: s.j.eskens@vu.nl.

You are invited to consult the Syllabus first for all your questions about this course. If the Syllabus does not answer your question, please email the course coordinator.

What is this course about?

This course teaches privacy and data protection law in the EU. We discuss the wide use of data about individuals in today's digital society, the diminishment of privacy due to business models and public services based on online tracking, and the role of the law in these developments.

Data-driven technologies bring opportunities and risks for individuals and societies. In this course, we discuss the main legal frameworks that can help address these risks and stimulate the use of data in commerce and government. While the law regulates the use of data about individuals to some extent, datafication also challenges existing legal rules and raise questions about whether current legal principles and doctrines are still suitable today. Furthermore, while data protection laws are already detailed, we discuss whether certain new technologies need new and even more specific rules.

In the EU, privacy and data protection are fundamental rights. The right to the protection of personal data is uniquely developed in secondary legislation. There are several secondary data protection instruments, including, among other things, the General Data Protection Regulation ('GDPR'), e-Privacy Directive, Law Enforcement Directive ('LED'), and Regulation for data processing by EU institutions ('EUDPR'). In addition to these EU law instruments, all countries in the EU are subject to the European Convention of Human Rights ('ECHR'), which guarantees the right to privacy.

We discuss the application of these different data protection laws and related case law of the Court of Justice of the EU ('CJEU'). Furthermore, we review case law of the European Court of Human Rights ('ECtHR') regarding surveillance regimes and their compatibility with the right to privacy.

At the end of this course, you will be able to:

- Identify what data protection instrument applies to the processing of personal data in a specific sector.
- Understand and apply the main EU privacy and data protection laws and the right to privacy as protected by the ECHR. The rules include, among others:
    - Data processing principles;
    - Rights of data subjects;
    - Obligations for controllers and processors;
    - Supervision and enforcement;
    - International data transfer.
- Analyse the role of privacy and data protection law in unequal balances of power between citizens and states, and consumers and big tech corporations.
- Evaluate whether existing EU data protection instruments are fit to deal with new technologies and support your evaluation with evidence.
- Formulate an original research question with regards to privacy and data protection law, and provide a well-structured, well-argued, and legally sound answer to that research question in writing.

How is this course taught?

This course has two modes of teaching:

- Lectures (on-campus, hybrid).
- Seminars (online).

The course consists of seven lectures taught by the course coordinator and guest lecturers. Because of the pandemic, there is no mandatory attendance for the lectures. The lectures are taught on-campus in a hybrid form, meaning that you may come to class on-campus or attend the lecture via Zoom. The lectures are recorded and published on Canvas afterwards. Please note that one lecture is taught fully online, as you can see in the course schedule below.

The course also offers four seminars where we practice applying the law and writing a research paper. The seminars are taught online via Zoom. Participation in the seminars is not mandatory, but it is highly recommended to attend them. The seminars are not recorded.

On Canvas, under Zoom, you can find the Zoom details to attend the lectures and seminars. To access a Zoom meeting, you need to be logged in to your Zoom account with your VU credentials.

Where do I find the reading materials?

There is no set textbook for this course. The reading materials for each week consists of journal articles, reports, book chapters, and other materials that are accessible via the University Library or are publicly available.

You can access online books, journals, and other sources in the library's collection with off-campus access. It is recommended to install the Lean Library browser extension, which is an easy way to access the materials you need.

The readings unavailable via the library or the open internet are uploaded to this Canvas page.

You can find case law by the CJEU with EUR-lex and case law by the ECtHR with HUDOC.

If you are looking for additional literature for your research paper, I advise you to consult this list of law databases the University Library provides.

Some privacy and data protection law journals, which you can access via the University Library:

- Computer Law & Security Review.
- European Data Protection Law Review.
- European Journal of Law and Technology.
- Global Privacy Law Review.
- International Data Privacy Law.
- International Review of Law, Computers & Technology.
- Journal of Intellectual Property, Information Technology and E-Commerce Law (Jipitec).
- SCRIPTed.
- Surveillance & Society.

What is the course schedule?

Week					
1	7 Feb 13:30		No teaching		
	10 Feb 15:30	Lecture 1	Introduction	Campus	Eskens
2	14 Feb 13:30	Seminar 1	Practising with GDPR	Online	Eskens
	17 Feb 15:30		No teaching		
3	21 Feb 13:30	Lecture 2	Key GDPR rules	Online	Eskens
	24 Feb 13:30	Lecture 3	GDPR enforcement	Campus	Eskens
4	28 Feb 13:30	Seminar 2	Practising with GDPR	Online	Eskens
	3 Mar 15:30	Lecture 4	Mass surveillance	Campus	Eskens
5	7 Mar 13:30	Lecture 5	International data transfers	Campus	Van Mil
	10 Mar 15:30	Seminar 3	Practising with writing	Online	Eskens
6	14 Mar 13:30	Lecture 6	Smart borders	Campus	Brouwer
	17 Mar 15:30	Seminar 4	Practising with writing	Online	Eskens
7	21 Mar 13:30		No teaching		
	24 Mar 15:30	Lecture 7	Looking beyond the GDPR	Campus	Eskens
8	28 Mar-1 Apr	Exam week	Research paper		
			Complete portfolio		

All lectures that are taught on-campus can also be followed live via Zoom!

What do I need to prepare for each lecture and seminar?

The mandatory reading for each lecture might seem like a lot. However, you need to read strategically. Always start with reading the assigned legal provisions. Then, use the reading materials to improve your understanding of these provisions and reflect critically on them. In particular, you do not need to read a court case entirely. Find out what the case is about and how it relates to the law, and then see what the court decided.

You do not need to prepare for the seminars. Just come by and participate!

10 Feb, lecture 1. Introduction to the course and the law

Information about individuals is used on a large scale to sell goods and services, make decisions about persons, and monitor populations. In this lecture, we discuss the wide range of data-driven technologies employed by the public and private sectors to deliver public services and do business. We debate the opportunities and risks of increasing datafication of societies. In the EU, a set of data protection laws regulates the processing of personal data to protect individuals and stimulate the free flow of data. We review the scope of these different instruments and then zoom in on the General Data Protection Regulation ('GDPR'). Who or what does the GDPR protect, and who should comply with its rules? Furthermore, in which areas of life does the GDPR apply, and where in the world do organisations need to follow its rules?

Mandatory reading:

- Articles 1 to 4 GDPR.
- Christl, W., 'Corporate surveillance in everyday life' (Cracked Labs, 2017).
    - This report comes as a webpage and PDF. It is enough to read the webpage.
- Finck, M., 'Cobwebs of control: the two imaginations of the data controller in EU law', *International Data Privacy Law*, 11:4 (2021), 333–47.

- Purtova, N., ‘The law of everything. Broad concept of personal data and future of EU data protection law’, *Law, Innovation and Technology*, 10:1 (2018), 40–81.
- CJEU 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994.
  - This case concerns the concept of ‘personal data’.
- CJEU 6 November 2003, *Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596.
  - This case concerns the household exemption.

Voluntary reading:

- Kuner, C., L. A. Bygrave, C. Docksey, and L. Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2018).
  - For each GDPR provision that you need to read, I advise you to consult the chapter in this book on that particular provision.
- Kuner, C., L. A. Bygrave, C. Docksey, L. Drechsler, and L. Tosoni, *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update* (Oxford University Press, 2021).
  - This book updates several chapters from the Kuner and others (2018) book.
- Mahieu, R., J. van Hoboken, and H. Asghari, ‘Responsibility for data protection in a networked world: on the question of the controller, “effective and complete protection” and its application to data access rights in Europe’, *JIPITEC*, 10:1 (2019).

14 Feb, seminar 1. Practising with the GDPR

During this seminar, we practise with the scope of the GDPR, as discussed in the first lecture. You may work on your own or in groups on cases where the question is: does the GDPR apply to these facts? After that, we discuss the cases with the group. We also practise finding case law and additional materials needed to interpret the rules of the GDPR.

21 Feb, lecture 2. Key rules of the GDPR

The GDPR has 99 articles and 173 recitals that explain the binding provisions. In this lecture, we discuss the key rules of the GDPR, which almost every technology lawyer will encounter in their practice. Last week we saw that the GDPR covers personal data processing and when and where it applies. This week we discuss the main principles of data processing and the requisites for lawful processing. Some of these principles are even stricter for special categories of data. The GDPR is famous and feared for the rights it gives to data subjects, although it turns out that it might be difficult to exercise your rights in practice. Finally, we discuss the obligations imposed by the GDPR on controllers and processors.

Mandatory reading:

- Articles 5 to 43 GDPR.
- Ausloos, J., and P. DeWitte, ‘Shattering one-way mirrors: Data subject access rights in practice’, *International Data Privacy Law*, 8:1 (2018), 4–28.
- Hahn, I., ‘Purpose limitation in the time of data power: Is there a way forward?’, *European Data Protection Law Review*, 7:1 (2021), 31–44.
- Tzanou, M., ‘The unexpected consequences of the EU right to be forgotten: Internet search engines as fundamental rights adjudicators’, in M. Tzanou (ed.), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, 2018).
- CJEU [GC] 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317.
  - This case concerns the ‘right to be forgotten’.
- CJEU [GC] 24 September 2019, *Google v. CNIL*, C-507/17, ECLI:EU:C:2019:772.
  - This case concerns the global exercise of the right to be forgotten.

Voluntary reading:

- Ausloos, J., 'The right to erasure: Safeguard for informational self-determination in a digital society?' (KU Leuven, 2018).
- Varon, J., and P. Peña, 'Artificial intelligence and consent: a feminist anti-colonial critique', *Internet Policy Review*, 10:4 (2021).

24 Feb, lecture 3. Supervision and enforcement of the GDPR

One of the main differences between the GDPR and its predecessor, the Data Protection Directive, is the strict system of supervision and enforcement of the GDPR. In this lecture, we discuss the crucial role of Data Protection Authorities ('DPAs'; in the GDPR: 'supervisory authorities') and the European Data Protection Board ('EDPB') within this system. Under the GDPR, DPAs can impose high fines. Furthermore, DPAs have a lot of power in interpreting the open norms of the GDPR. In addition to actions on the initiative of DPAs, individuals can lodge complaints and go to court to exercise their data protection rights. Activists like Max Schrems and Johnny Ryan use their data protection rights to change how big tech firms collect, analyse, and sell our data. Likewise, groups of individuals such as Uber and Ola drivers collectively exercise their rights to address the power of big tech firms. We reflect on these strategies and consider the right way forward to ensure that the GDPR is adhered to in practice.

Mandatory reading:

- Articles 51 to 84 GDPR.
- Hugues, B.-D., and W. G. Voss, 'EU General Data Protection Regulation sanctions in theory and in practice', *Santa Clara High Technology Law Journal*, 37:1 (2021).
- Hajduk, P., 'The powers of the supervisory body in the GDPR as a basis for shaping the practices of personal data processing', *Review of European and Comparative Law*, 45 (2021), 57–76.
- Toh, J., 'Empowering workers through digital rights', *Digital Freedom Fund*.
- CJEU [GC] 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125.
  - This case concerns the independence of supervisory authorities.
- CJEU [GC] 15 June 2021, *Facebook Ireland and others*, C-645/19, ECLI:EU:C:2021:483.

Voluntary reading:

- Barros Vale, S., G. Zanfir-Fortuna, and R. van Eijk, 'Insights into the future of data protection enforcement: Regulatory strategies of European Data Protection Authorities for 2021-2022' (Future of Privacy Forum, 2021).
- Cochrane, L., L. Jasmontaite-Zaniewicz, and D. Barnard-Wills, 'Data Protection Authorities and their awareness-raising duties under the GDPR: The case for engaging umbrella organisations to disseminate guidance for small and medium-size enterprises', *European Data Protection Law Review*, 6:3 (2020), 352–64.
- Svenonius, O., and E. Tarasova, '"Now we are struggling at least": Change & continuity of surveillance in post-communist societies from the perspective of Data Protection Authorities', *Surveillance & Society*, 19:1 (2021), 53–68.

28 Feb, seminar 2. Practising with the GDPR

During this seminar, we practise with the key rules of the GDPR, as discussed in the second lecture. You may work on your own or in groups on cases where the question is: how does this GDPR rule apply to these facts? What rights does the data subject have, and how can the controller meet its obligations?

03 Mar, lecture 4. Mass surveillance and data retention

In 2013, Edward Snowden revealed that the National Security Agency of the U.S. engaged in global surveillance and that many other intelligence services worldwide were also collecting internet and telephone data on an unprecedentedly large scale. States argue that they need to conduct mass surveillance to protect national security. Many governments have therefore given their intelligence services more and more surveillance powers. Mass surveillance interferes with the right to privacy and data protection but may be lawful under certain conditions. In this lecture, we analyse the evolution of case law of the ECtHR and compare this with recent judgments of the Court of Justice of the EU regarding data retention. We will see how the case law of the two European courts follows a different approach, with the one more deferential towards states and the other stricter.

Mandatory reading:

- Article 8 ECHR.
- Articles 7, 8, and 52(1) CFEU.
- Article 15(1) e-Privacy Directive.
- Eskens, S. 'The ever-growing complexity of the data retention discussion in the EU: An in-depth review of *La Quadrature du Net and others* and *Privacy International*', draft paper (2022).
    - I ask you not to share this paper with other people without my consent.
- Van der Sloot, B., 'Is the human rights framework still fit for the big data era? A discussion of the ECtHR's case law on privacy violations arising from surveillance activities', in S. Gutwirth, R. Leenes, and P. De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer Netherlands, 2016), pp. 411–36.
- CJEU [GC] 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
- CJEU [GC] 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.
- ECtHR [GC] 25 May 2021, *Centrum för Rättvisa v. Sweden*, 35252/08.
    - Focus on the question whether there was a violation of article 8 ECHR and why (not).
- ECtHR [GC] 25 May 2021, *Big Brother Watch and other v. the United Kingdom*, 58170/13, 62322/14 and 24960/15.
    - Focus on the question whether there was a violation of article 8 ECHR and why (not).

Voluntary reading:

- Murphy, M. H., 'Algorithmic surveillance: The collection conundrum', *International Review of Law, Computers & Technology*, 31:2 (2017), 225–42.
- Epstein, R. A., 'The ECJ's fatal imbalance: its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices', *European Constitutional Law Review*, 12:2 (2016), 330–40.

07 Mar, lecture 5. International data transfer

This lecture is taught by Jurriaan van Mil, Junior Associate at Stibbe Amsterdam.

Most big tech companies are in the U.S. When they collect personal data about persons in the EU and send these data to the U.S. or another non-EU country, they need to comply with a complex regime in the GDPR. The transfer of personal data to a non-EU country (also called 'third country') may take place based on several different regimes, such as an adequacy decision from the European Commission, binding corporate rules, or standard contractual clauses. However, several procedures started by Maximilian Schrems before the Court of Justice of the EU (see the previous lecture) have limited the options for organisations to transfer data out of the EU. In this lecture, we discuss these international transfer regimes, including the now-defunct Safe Harbour and Privacy Shield.

Mandatory reading:

- Articles 44 to 50 GDPR.
- Kuner, C., 'Territorial scope and data transfer rules in the GDPR: realising the EU's ambition of borderless data protection' (University of Cambridge Faculty of Law Research Paper No. 20/2021).
- EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
- EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
- EDPB, Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfer as per Chapter V of the GDPR.
- Commission Implementing Decision of 4 June 2021 on standard contractual clauses.
- CJEU [GC] 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.
- CJEU [GC] 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559.

Voluntary reading:

- EDPB, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.
- Breitbarth, P., 'A risk-based approach to international data transfers', *European Data Protection Law Review*, 7:4 (2021), 539–49.
- Gulczyńska, Z., 'A certain standard of protection for international transfers of personal data under the GDPR', *International Data Privacy Law*, 11:4 (2021), 360–74.
- Corrales Compagnucci, M., M. Aboy, and T. Minssen, 'Cross-border transfer of personal data after Schrems II: supplementary measures and new standard contractual clauses (SCCs)', 2021.
- Jurcys, P., M. Corrales Compagnucci, and M. Fenwick, 'The future of international data transfers: managing new legal risk with a "user-held" data model', 2022.
- For a critical view on Guidelines 05/2021, see:
  - Kuner, C., 'Exploring the awkward secret of data transfer regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR', *European Law Blog*, 2021.
  - Yakovleva, S., 'GDPR transfer rules vs rules on territorial scope: A critical reflection on recent EDPB Guidelines from both EU and international trade law perspectives', *European Law Blog*, 2021.

10 Mar, seminar 3. Practising with writing

During this seminar, we practice writing a research question, as you need to do for your research paper. In the first twenty minutes of the class, you draft a research question related to the previous lectures. You then discuss your research question in breakout rooms. After that, we discuss the results together.

14 Mar, lecture 6. Smart borders: data protection and access to effective remedies

This lecture is taught by Evelien Brouwer, Assistant Professor Public Law and Technology at Utrecht University.

This lecture addresses current (and proposed) measures of data surveillance at the external borders of the EU for immigration control and security reasons, including the use of large-scale databases, profiling and risk analysis, and in the future perhaps even lie-detectors. During this lecture, we discuss the development of 'smart borders' and interoperability from the perspective of both effectiveness and human rights (including data protection, non-discrimination, and effective remedies).

Mandatory reading:

- Article 47 CFEU.
- Articles 5 to 9, 21 and 22, and 77 to 79 GDPR
  - These articles are relevant for the prohibition of automated decision-making.
- European Commission, Proposal for an Artificial Intelligence Act.
  - Read in particular articles 5 to 7 of the proposal.
- Brouwer, E., 'Large-scale databases and interoperability in migration and border policies: The non-discriminatory approach of data protection', *European Public Law*, 26:1 (2020), 71–92.
- Leese, M., S. Noori, and S. Scheel, 'Data matters: the politics and practices of digital border and migration management', *Geopolitics*, 27:1 (2022), 5–25.
- De Hert, P., and G. Lazcoz, 'Radical rewriting of Article 22 GDPR on machine decisions in the AI era', *European Law Blog*, 2021.
- CJEU [GC] 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.
- CJEU [GC] 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.
- CJEU 24 November 2020, *R.N.N.S and K.A.*, C-225/19 and C-226/19, ECLI:EU:C:2020:951.

17 Mar, seminar 4. Practising with writing

During this seminar, we practise structuring and organising a paper. You view anonymised papers from last year's course. In breakout rooms, you evaluate the structure of these papers, identify strengths, and propose improvements. After that, we discuss your insights together. You also learn to write down your references with an appropriate reference style.

24 Mar, lecture 7. Looking beyond privacy and data protection law

Throughout this course, we have discussed how privacy and data protection laws offer individuals (at least some) control over their personal data and constrain the public and private sector in the way they collect and analyse personal data. In this lecture, we reflect on the strengths and weaknesses of privacy and data protection law. We consider how the right to privacy may harm women and whether the tendency to frame new technologies mainly as privacy and data protection issues may risk us overlooking other values.

The lecture comes with a long list of readings. You are invited to pick two or three articles that interest you or read other critical articles you found yourself.

Suggested reading:

- Allen, A. L., 'Privacy at home', in *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield, 1988).
- Arora, P., 'Decolonising privacy studies', *Television & New Media*, 20:4 (2019), 366–78.
- Bellanova, R., 'Digital, politics, and algorithms', *European Journal of Social Theory*, 20:3 (2016), 329–47.

- Geradin, D., T. Karanikioti, and D. Katsifis, ‘GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech’, *European Competition Journal*, 17:1 (2021), 47–92.
- Hong, S., ‘Criticising surveillance and surveillance critique: Why privacy and humanism are necessary but insufficient’, Surveillance & Society, 15:2 (2017), 187–203.
- Keller, P., ‘The reconstruction of privacy through law: a strategy of diminishing expectations’, *International Data Privacy Law*, 9:3 (2019), 132–52.
    - Keller argues that ‘the explanation for this long running failure [of data protection law] lies substantially in the wider political economy of information law, which continues to shape and limit the capacities of privacy and data protection law.’
- Sharon, T., ‘Beyond privacy: there are wider issues at stake over Big Tech in medicine’, *OpenDemocracy*, 2022.
    - Sharon argues that ‘our focus on privacy may be unwittingly enabling, rather than hindering, the continued expansion of Big Tech into new sectors.’
- Van de Waerdt, P. J., ‘Information asymmetries: recognizing the limits of the GDPR on the data-driven market’, *Computer Law & Security Review*, 38 (2020).
    - Van de Waerdt argues that the GDPR is ‘unable to mitigate these information asymmetries, nor would it be able to provide for effective transparency, since it does not account for the unique characteristics of the data-driven business model.’
- Wagner DeCew, J., ‘The feminist critique of privacy: past arguments and new social understandings’, in B. Roessler and D. Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press, 2015), pp. 85–103.
- Yeung, K., and L. A. Bygrave, ‘Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship’, *Regulation & Governance*, 16:1 (2022), 137–55.
- Zarsky, T. Z., ‘Incompatible: the GDPR in the age of big data’, *Seton Hall Law Review*, 47:4 (2016), 995–1020.

How will I be examined for this course?

Examination for the course has two components:

- Portfolio.
- Research paper.

You do not need to register for these exam components.

Portfolio

Throughout the course, you build a portfolio of small assignments each week. The purpose of the portfolio is to stimulate you to engage with the materials every week and explore your interests within the broad field of privacy and data protection. The portfolio assignments are meant to be fun, and you are encouraged to use your creativity in writing and formatting the assignments. You may write in a more personal, non-academic manner and use images and decorative elements.

The process:

- Each week, you hand in your portfolio assignment for that week via Assignments on Canvas.
- You bundle your five assignments into one PDF at the end of the course. This is your complete portfolio.
- You hand in your complete portfolio via Assignments on Canvas.

- You receive a grade for your complete portfolio.

Portfolio requirements:

- Deadline:
  - Individual assignments: each week, the deadline is the Sunday of that week at 16:00 CET.
  - Complete portfolio: 3 April 2022 at 16:00 CET.
- Length of each individual assignment: around half a page of text.
- There are six portfolio assignments, but you can miss one. That means that your portfolio needs to contain five items towards the end of the course.
- Weighting: 30%.
- Include only your student number in the portfolio and not your name or other identifying information.

You can find the portfolio assignments for each week on Canvas under Assignments. You can also find a rubric for the complete portfolio when clicking on that button under Assignments on Canvas. The rubric tells you how we grade your complete portfolio.

Research Paper

You finish the course by writing a research paper on a chosen topic. For the research paper, you formulate your own research question on your chosen topic and then provide a well-structured, well-argued, and legally sound answer to that research question. The idea of the research paper is that you do your own research on a data protection law topic of your interest while building on and demonstrating the knowledge you obtained through the course. On Canvas, under Assignments, you can find a list of topics from which you must choose.

Research paper requirements:

- Deadline: 3 April 2022 at 16:00 CET.
- Word count: 1500 (with a 10% margin).
  - Word count includes headings but excludes the cover page and footnotes.
- Weighting: 70%.
- Include a cover page, with:
  - Title of the paper.
  - Student number.
  - Number of words.
- References according to a consistent and complete reference style.
- Submit in PDF.
- Include only your student number on the research paper and not your name or other identifying information.

You can find a rubric for the research paper when clicking on the research paper button under Assignments on Canvas. The rubric tells you how we grade your research paper and helps you organise your paper.

Examination policy

You may be sick before a deadline, or important things happen in your life that take up your attention and energy. If you inform me, the course coordinator, at least 24 hours in advance of a deadline, we can adjust the deadline for you without any further questions asked. If you get sick or something happens within 24 hours before a deadline, we can change the deadline for you upon presenting a doctor’s note or other documentation.

You may take a resit for the complete portfolio and the research paper. If you take a resit for the complete portfolio, you must submit an entirely new portfolio. Likewise, if you take a resit for the research paper, you need to choose a new topic from the list and write a completely new paper. When you partake in a resit, your last obtained result counts.

You are not allowed to conduct plagiarism. On Canvas under Modules, you can find the Plagiarism Handbook that sets out what is plagiarism and how to prevent it. If you conduct plagiarism, your complete portfolio or research paper is rejected, and in severe cases, we notify the Examination Board.

The box on Canvas to hand in your complete portfolio or research paper closes precisely at the deadline. To ensure that you can successfully submit your work in time, I advise you to start the submission process at least fifteen minutes before the deadline. Remember that the complete portfolio and research paper need to be submitted in PDF format.