



INTERNET PRIVACY AND EU DATA PROTECTION

Seminar I.

Introduction. History, Context and Background of EU DP Law. And DP Institutions

prof. dr. Gerrit-Jan Zwenne

October 30th, 2024



lecturers



G.J. (Gerrit-Jan) ZWENNE
Full Professor Leiden University &
Open University | Partner Pels Rijcken
& Droogleevers Fortuijn N.V.



B.H.M. (Bart) CUSTERS
Full Professor Leiden
University



H.U. (Helena) VABREC
Guest Researcher eLaw
Legal Counsel InstaCart



P.J. (Peter) HUSTINX
non-executive director ICO, Board
of Directors IAPP, former chair of
Dutch DPA and EDPS



Daniel WINTERMANS
Autoriteit
persoonsgegevens



A.M. (Alan) SEARS
Researcher & Lecturer
at eLaw



O.M. (Oliver) TUAZON
Researcher at eLaw



quick overview

30 October 9:15-13:00
 I. Introduction. History, Context and Background of EU DP Law. DP Institutions *prof. Gerrit-Jan ZWENNE*
 II. Key concepts of EU Data Protection Law and its Applicability *prof. Gerrit-Jan ZWENNE*
 III. The significance of EU DP law in Europe and the Rest of the World *Peter HUSTINX*

4 November 9:15 – 11:00
 IV. The Main Principles and Rules relating to Data Protection *prof. Gerrit-Jan ZWENNE*

6 November 9:15-11:00
 V. The Data Protection Officer or DPO *prof Gerrit-Jan ZWENNE*
 23 November 14:15-15:15
 VI. IoT, Datafication, Big Data, AI, Machine Learning etc. *prof Gerrit-Jan ZWENNE*

11 November 9:15-11:00
 VII. Data subject rights and controller transparency obligations *prof. Bart CUSTERS*

13 November 9:15-11:00
 VIII. Data Protection Authorities, *Daniel WINTERMANS*

18 November 9:15-11:00
 XI. Workshop on the Right to be Forgotten *Alan M. SEARS*

22 November 13:15-17:00
 XI Third Country Data Transfers *Helena VRABEC*
 XI Genetic Data *Oliver TUAZON*
 XII Exam Training *Alan M. SEARS*

★ 29 November 9:00-12:00
Written Exam

★ 9 December
written group assignment due!

literature



recommended literature is not required reading



group assignment

WARNING! use of LLM's could be considered plagiarism..!

- short paper, approx. 3000 - 4000 words
- pre-defined structure & template
- explains the facts, questions and significance of a specific CJEU-decision

§1 facts of the case in a concise manner (approx. 500 words)

§2 discusses the legal questions the Court had to answer and its answers (approx. 500 words)

§3 provides context (e.g. relation with other relevant court decisions or literature), explains the significance of the decision, its relation with other court decisions, and allows the author to give his or her opinion on whether or not it's a good or bad decision, the implications etc. (2000-3000 words)





WARNING! use of LLM's could be considered plagiarism..!

ChatGPT: What is possible and what is allowed?

At the moment a lot of discussion surrounds ChatGPT, an advanced chatbot which uses Artificial Intelligence (AI). ChatGPT is based on a Large Language Model (LLM) and has been trained using an enormous amount of text, providing it with knowledge of grammar, semantics and contextual nuances. The program can answer questions, give information, make suggestions and help create text. It is however important to know that software like ChatGPT is in ongoing development, and that using a chatbot comes with constraints and challenges.

What is allowed?
Students can use ChatGPT as a sparring partner. This means that ChatGPT can be a useful tool during the beginning stages of your research. For example, it can help you whilst brainstorming and it can help you search for information. Be aware that ChatGPT does not always give you factual information. This means that you have to check the validity of its replies yourself. ChatGPT can also help you structure your text.

What is not allowed?
It is not allowed to let ChatGPT write your text, or to let it rewrite an already existing text. This is seen as plagiarism, as your text will be based on someone else's words and the original source will not be cited. ChatGPT is good with tone and structure, but lacks interpretative skills and cannot understand the text it processes or generates. Sometimes the tool also fabricates references and sources. These are not usable for your research.

What do you want to learn?
It is important to remind yourself of the reason why you are studying. It is unlikely that letting a chatbot do your work will improve the skills you're trying to gain. In addition, transparency is one of the core values of science. It is therefore crucial to let people know if and how you used ChatGPT in your work. Talk to your teacher or supervisor about what they accept in terms of you using ChatGPT and how you can specify this.

exam

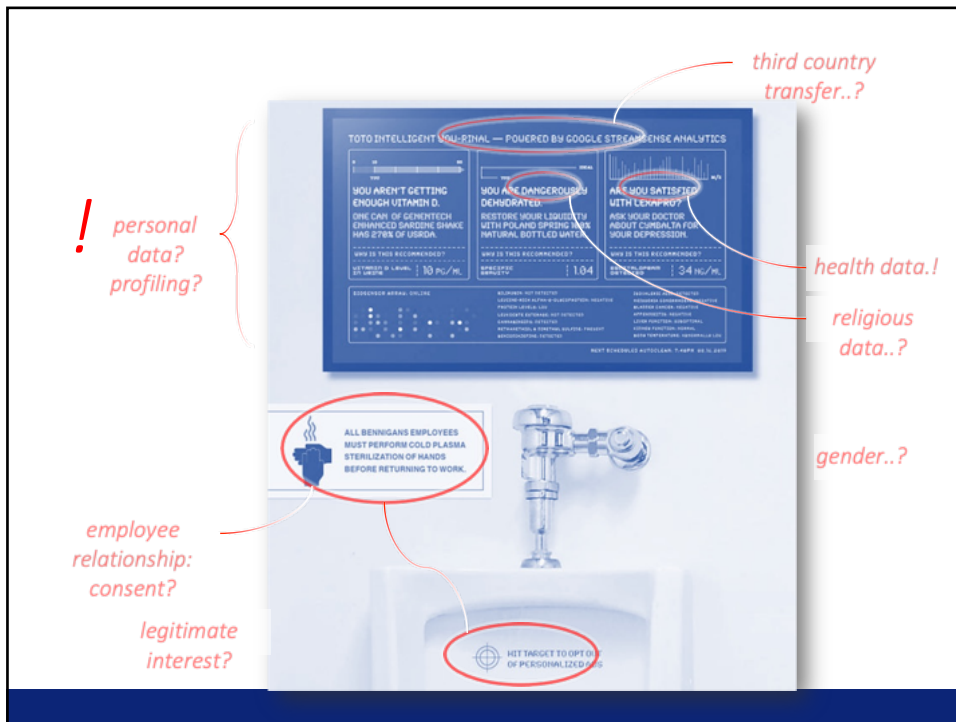
- 29 November, 9:00-12:00
- SPORTCENTRUM
- written, through Ans (on laptops)
- probably three or four questions (with sub-questions!)

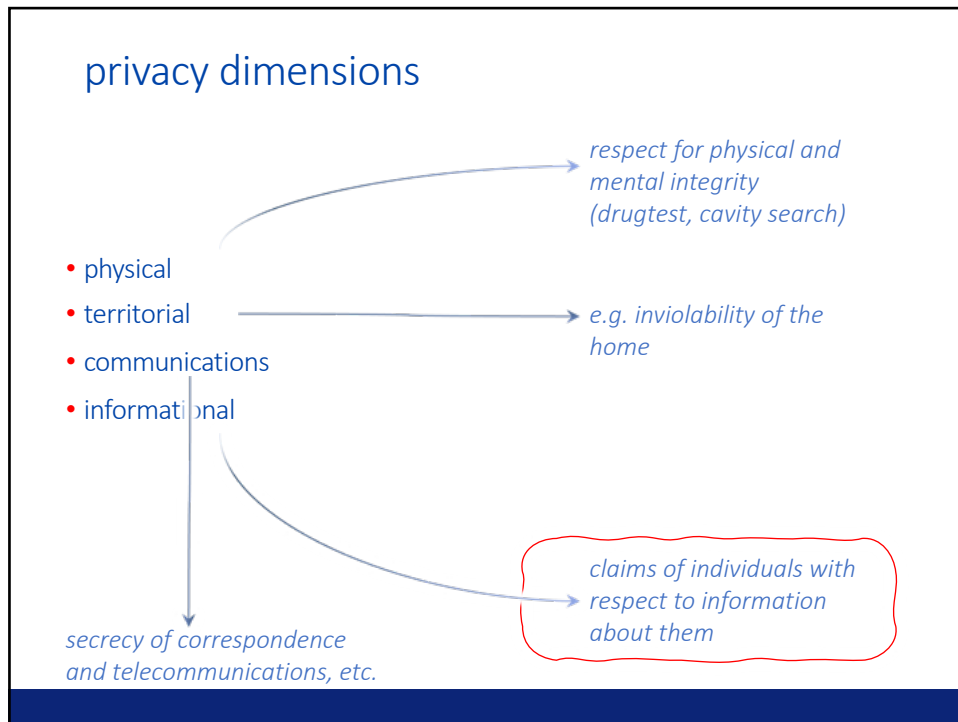


preliminary remarks

introduction

Total U-rinal





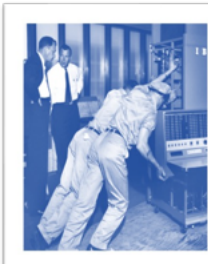

history



“The Right to Privacy”
Warren and Brandeis
 Harvard Law Review.
 Vol. IV December 15, 1890 No. 5
 THE RIGHT TO PRIVACY¹.

¹It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent, much more when received and approved by usage. — Wilson, J., in *Miller v. Taylor*, 4 Burr. 2303, 2312.

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the “right to life” served only to protect the subject from injury in its various forms; liberty meant freedom from actual seizure; and the right to recover, secured to the individual his lands and his cattle. Later, there came a recognition of

1 Y 3426 A
425

Gesetz- und Verordnungsblatt für das Land Hessen - Teil I

1930	Ausgaben zu Wiesbaden am 12. Oktober 1930	Nr. 41
Teil	Inhalt	Seite
7. 10. 30	Datenschutzgesetz GVBl. II 20-19	425
7. 10. 30	Gesetz zur Änderung beamtenrechtlicher und beamtengerichtlicher Vorschriften GVBl. II 21-20	428
7. 10. 30	Gesetz über verordnungsrechtliche Leistungen für Beamte GVBl. II 22-18	433
7. 10. 30	Zweites Gesetz zur Änderung des Hessischen Personalvertretungsgesetzes Anderl. GVBl. II 23-2	434
7. 10. 30	Gesetz über die Anwartschaftsbefreiung und den Ehrenlohn der ehrenamtlichen Bürgermeister und der ehrenamtlichen Kassaverwalter der Gemeinden GVBl. II 24-11	435
7. 10. 30	Gesetz zur Änderung des Hessischen Archivgesetzes Anderl. GVBl. II 25-3	438
7. 10. 30	Drittes Gesetz zur Änderung des Gerichtsverfassungsgesetzes Anderl. GVBl. II 25-10	439
7. 10. 30	Gesetz zur Änderung des Hessischen Schiedsmannengesetzes Anderl. GVBl. II 26-1	440
7. 10. 30	Gesetz über die Befreiung zur Bestimmung von Zustellungsstellen nach der Kreisverordnung GVBl. II 27-11	441
7. 10. 30	Gesetz über die Wahlgesetze GVBl. II 28-21	441

Der Landtag hat das folgende Gesetz beschlossen:

Datenschutzgesetz*)
 Vom 7. Oktober 1930

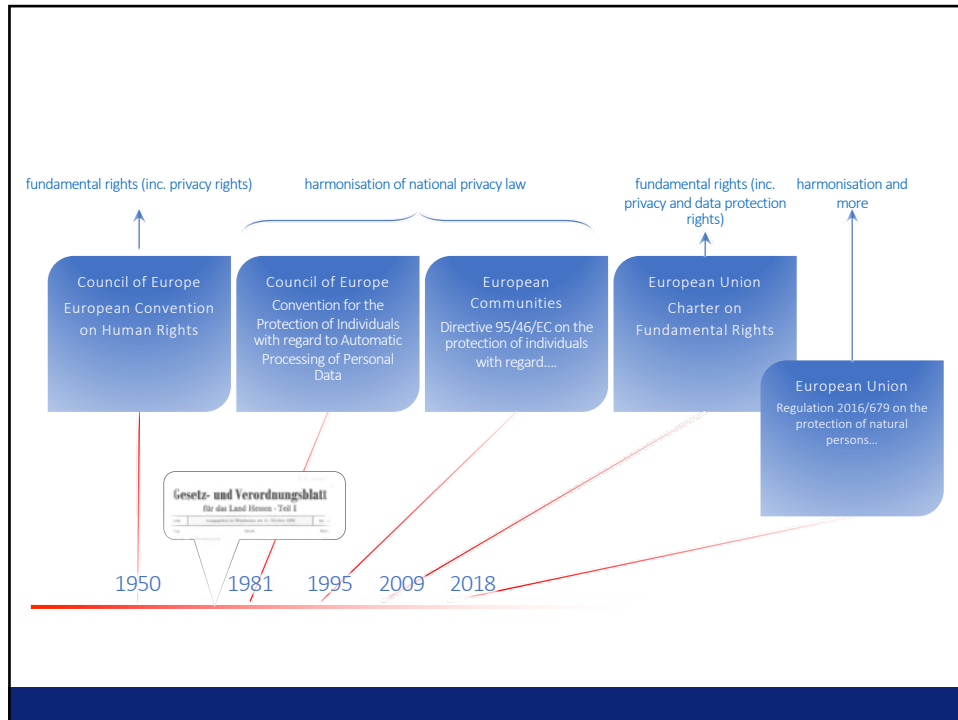
ERSTER ABSCHNITT
Datenschutz

§ 1
Bereich des Datenschutzes
 Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erzielten Datenergebnisse sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Ämtern und Stützungen des öffentlichen Rechts.

§ 2
Inhalt des Datenschutzes
 Die von Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu erheben, weiterzuführen und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, veröffentlicht, abgerufen oder vernichtet werden können. Dies ist durch geeignete personale und technische Vorkehrungen sicherzustellen.

§ 3
Datenspezifische
 (1) Dem mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen ist untersagt,

*) GVBl. II 20-19

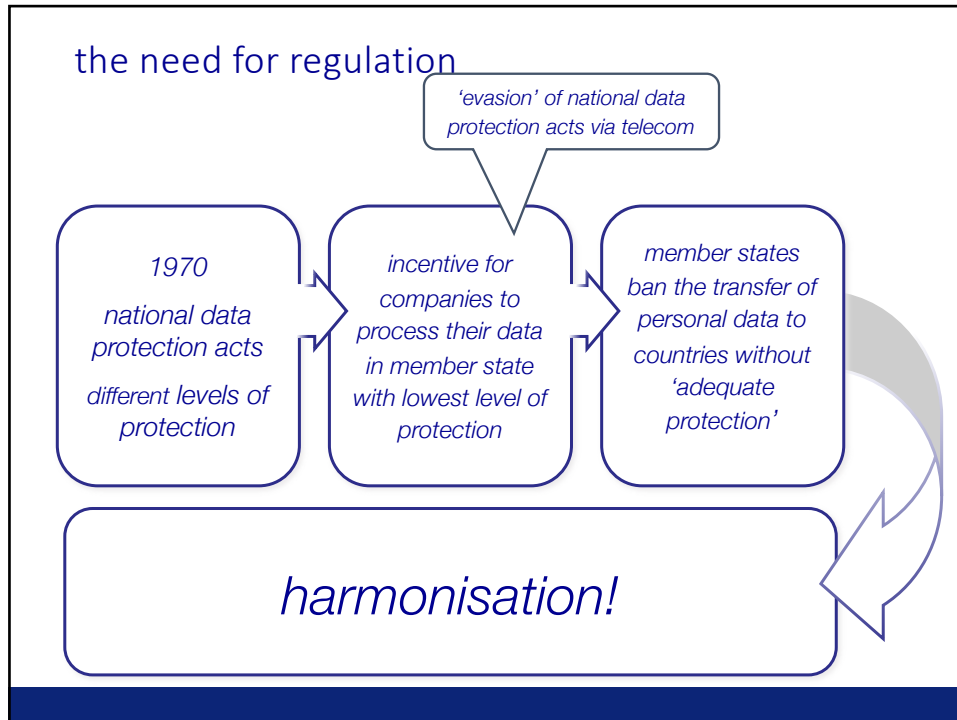


data processing 1960's



1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz





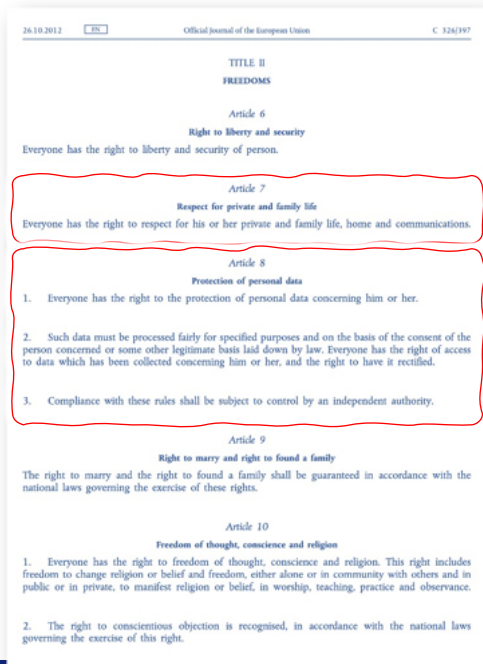
(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(13) [...] The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

General
Data
Protection
Regulation



EU Charter of Fundamental Rights (2000)



legal basis

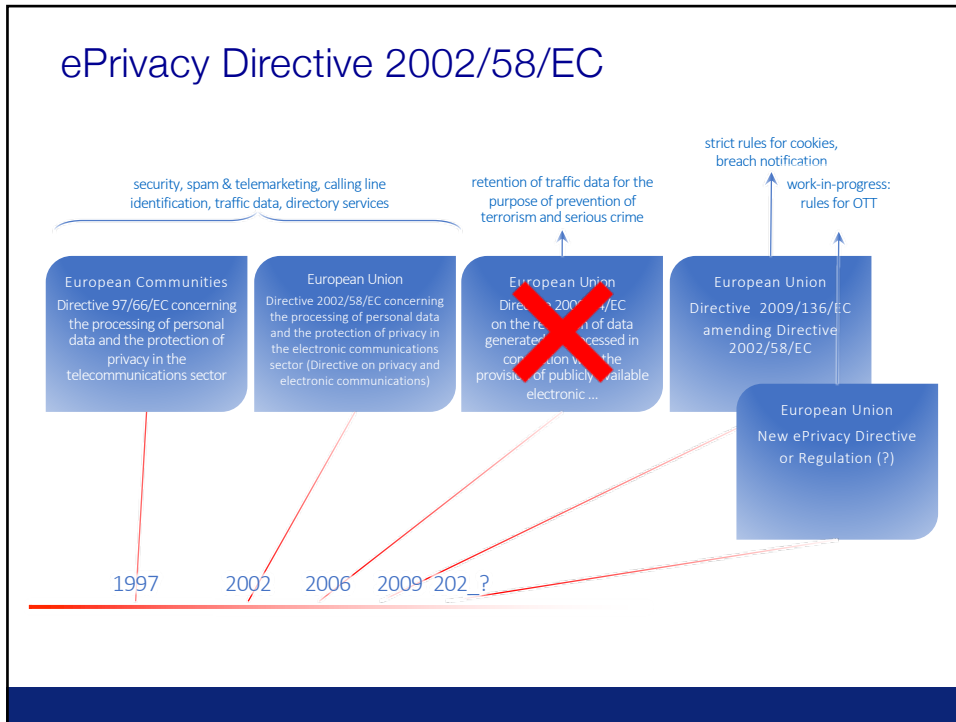
Article 16(2) TFEU

The European Parliament and the Council [...] shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. [...]

Article 114(1) TFEU

The European Parliament and the Council shall [...] adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

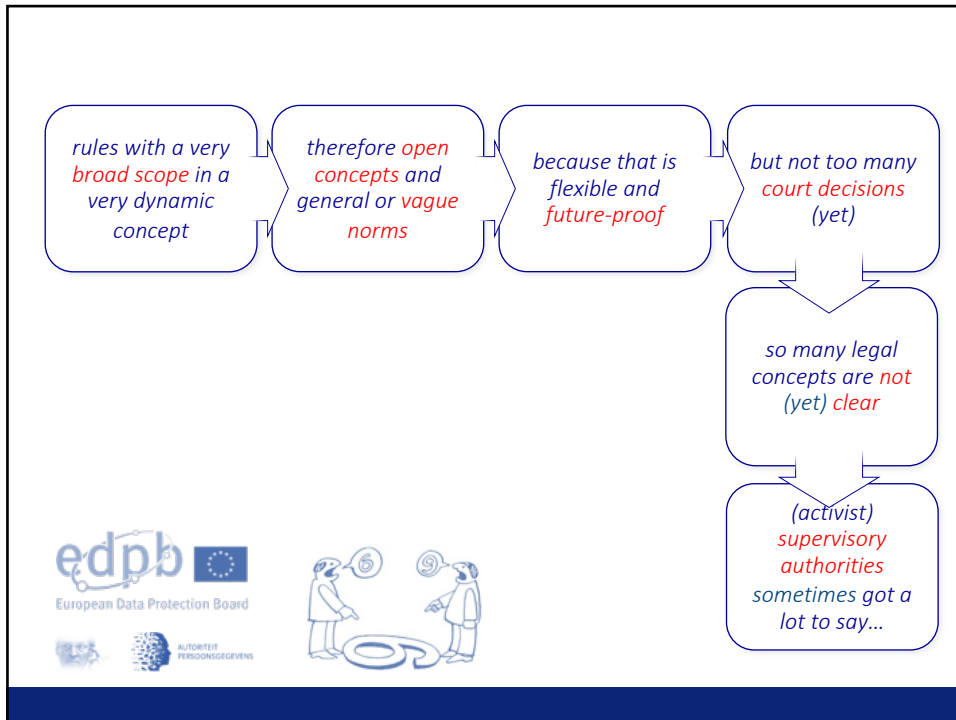




national DP-law

- special data and criminal data
- health care and social security
- exemptions for the press (freedom of information)
- establishment and organisation of the supervisory authority

In the Netherlands: GDPR Implementation Act (*Uitvoeringswet AVG* or *UAVG*)



QUESTIONS

1. When did the European Convention of Human Rights (ECHR) enter into force?

- A. 1946
- B. 1949
- C. 1953
- D. 1966

Question 1a preparation assignment questions

2. And what article of that Convention deals with privacy and data protection?

- A. Article 6
- B. Article 8
- C. Article 10
- D. Article 12

Question 1b preparation assignment questions





QUESTION

3. Why did policymakers and lawmakers in some European countries see the need for data protection law (data privacy law) in the 1960s and the early 1970s

- A. Because, at that time the ARPANET, a precursor of the internet, was created and subsequently specific DP-law was needed
- B. Because, particularly government and multinationals started using computers for processing personal data and as a result new threats to privacy emerged
- C. Because of Alan F. Westin's influential books on Privacy and Freedom (1967) and Databanks in a Free Society (1972)

Question 2 preparation assignment questions



QUESTION

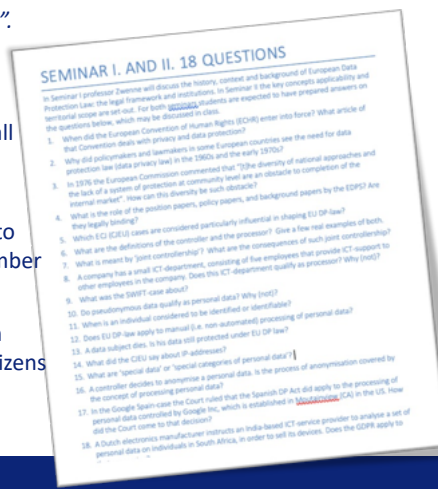
4. In 1976 the European Commission commented that

"[t]he diversity of national approaches and the lack of a system of protection at community level are an obstacle to completion of the internal market".

How can this diversity be such obstacle?

- A. Because companies don't have sufficient knowledge of all data protection rules in all member states
- B. Because member states that have data protection rules cannot allow companies to avoid these rules by using facilities in member states without these rules
- C. Because it is immoral that some European citizens are protected, and some other citizens are not

Question 3 preparation assignment questions





QUESTION

5. What is the role of the position papers, policy papers, guidelines and background papers published by WP29, EDPB and EDPS? Are they legally binding?

- A. The position papers, policy papers and background papers are not binding; the guidance is binding
- B. All documents published by these authorities are binding
- C. None of these documents are binding
- D. These documents only bind the authorities that published these

Question 4 preparation assignment questions



institutions



European Court of Human Rights (ECtHR)



broad interpretation of privacy
(art. 8 ECHR)

the concept of "private life" is a broad term not susceptible to exhaustive definition

e.g. S. & Marper v. UK 2008



Court of Justice of the EU (CJEU)



- Luxembourg
- highest authority on interpreting EU law
- national courts can ask CJEU advice on interpretation EU law

Lindqvist, Data Retention, Google Spain, Weltimmo, Schrems I and II, Breyer, GC/CNIL, Schrems I and II, etc.



COURT OF JUSTICE OF THE EUROPEAN UNION



independent supervisory authorities

CNIL, AP, GBA, etc.



- National: Data Protection Authorities (“DPAs”) or Supervisory Authorities (“SAs”)
- European Data Protection Board (“EDPB”) Advisory body: opinions, working documents etc.
- European Data Protection Supervisor (“EDPS”) Supervises processing by EU bodies (Reg 45/2001, art 41-48)

former “Article 29 Working Party” or “WP29”

QUESTIONS

1. Which ECJ (CJEU) cases are considered particularly influential in shaping EU DP-law?

- A. CJEU 13 May 2014, C-131/12, (Google Spain) and CJEU 24 September 2019, C-507/17 (Google/CNIL) and CJEU 24 September 2019 C-136/17 (GC/CNIL)
- B. CJEU 17 July 2014, C-141/12 and C-372/12 (IND) and CJEU 20 december 2017, C 434/16, (Nowak)
- C. CJEU 6 October 2015, C-362/14 (Schrems I)
- D. All of the above (and many more)





PRIVACY AND EU DATA PROTECTION

Seminar II.

Key concepts of EU Data Protection law and its applicability (incl. territorial scope)

prof. dr. Gerrit-Jan Zwenne

November 2nd, 2022



if I go to a pub one evening...

AG Bobek Opinion
6 October 2021,
C-245/20 X v AP

56. If I go to a pub one evening, and I share with four of my friends around the table in a public place (thus unlikely to satisfy the private or household activity exception [...]) a rather unflattering remark about my neighbour that contains his personal data, which I just received by email (thus by automated means and/or is part of my filing system), do I become the controller of those data, and do all the (rather heavy) obligations of the GDPR suddenly become applicable to me? Since my neighbour never provided consent to that processing (disclosure by transmission), and since gossip is unlikely ever to feature amongst the legitimate grounds listed in Article 6 of the GDPR, (30) I am bound to breach a number of provisions of the GDPR by that disclosure, including most rights of the data subject





program

next week

context

- *privacy and privacy law*
- *the need for harmonisation*

players

- *data subject*
- *controller*
- *processor*
- *DPA and DPO*

playing field

- *processing of personal data and filing system*
- *personal or household activities*
- *journalism*
- *the territorial scope*

rules of the game

- *processing grounds*
- *purpose limitation*
- *storage and retention*
- *special categories of data*



players

data subjects, controllers, processors, dpo's and dpa's



players

Art. 4 GDPR

data subject ('individual')

- an identifiable person (ie a natural person) who can be identified, directly or indirectly

controller

- controls the purposes and means of processing
- natural person, legal person, or government institution

processor


- processes data for the controller, without being directly under its authority

DPA (SA)

- authority overseeing the processing of personal data

DPO

- data protecting officer



“the controller” and “the processor”

the natural or legal person, public authority, agency or any other body which alone or jointly with others **determines purposes and means of the processing** of personal data.

a natural or legal person, public authority, agency or other body which processes personal data on **behalf of the controller**

Art. 4(7) and (8) GDPR



*The Working Party recognizes that the concrete application of the concepts of data controller and data processor is becoming **increasingly complex**. This is mostly due to the increasing complexity of the environment in which these concepts are used, and in particular due to a growing tendency, both in the private and in the public sector, towards **organisational differentiation**, in combination with the development of ICT and globalisation, in a way that may give rise to new and difficult issues and may sometimes result in a lower level of protection afforded to data subjects.*

who is in control..?

who determines retention terms?

who decides on DSAR's

who decides on outsourcing?

which party enters into contracts with the data subjects

who notifies a data breach?





CJEU 5 June 2018, C-210/16,
ECLI:EU:C:2018:388 *Wirtschaftsakademie*

- in view of the objectives of DP-law, the concept of 'controller' must be interpreted broadly
- *Wirtschaftsakademie* created a fanpage on Facebook and is considered a joint controller with Facebook, as they do have a part to play in the means and purposes of processing personal data.
- A key factor in this finding is that non-Facebook users could be brought to the Facebook fan-page of *Wirtschaftsakademie*, which may otherwise not have been within Facebook's sphere of influence



CJEU 29 July 2019, C-40/17
ECLI:EU:C:2019:629 *FashionID*

- in view of the objectives of DP-law, the concept of 'controller' must be interpreted broadly
- *Fashion ID* can be considered to be a controller jointly with Facebook Ireland in respect of the operations involving the collection and disclosure by transmission to Facebook Ireland of the personal data at issue
- as *Fashion ID* and Facebook Ireland determine jointly the means and purposes of those operations.

CJEU 10 July 2018, C-25/17,
ECLI:EU:C:2018:551 *Jehova's witnesses*

- [T]he collection of personal data relating to persons contacted and their subsequent processing help to achieve the objective of the Jehovah's Witnesses Community, which is to spread its faith and are, therefore, carried out by members who engage in preaching for the purposes of that community.
- Furthermore, not only does the Jehovah's Witnesses Community have knowledge on a general level of the fact that such processing is carried out in order to spread its faith, but that community organises and coordinates the preaching activities of its members, in particular, by allocating areas of activity between the various members who engage in preaching.
- it appears that the Jehovah's Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participates, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted...



CJEU 5 December 2023, C-683/21,
ECLI:EU:C:2023: *Covid19 App*

- the creation of the mobile application at issue was commissioned by the NVSC and was intended to implement the objective assigned by that entity, namely the management of the COVID-19 pandemic by means of an IT tool for registering and monitoring the data of persons exposed to the COVID-19 virus.
- For that purpose, the NVSC had envisaged that the personal data of users of the mobile application at issue would be processed.
- Furthermore, it is apparent from the order for reference that the parameters of that application, such as the questions asked and their wording, were adapted to the needs of the NVSC and that that entity played an active role in their determination.





- a Facebook user uploads photo's to her profile page or feed
- the tax authorities require that you submit your income details in an electronic form and via their online tax portal
- to discover and prevent health insurance fraud municipalities and insurers construct a fraud detection system: each participant uploads data ('signals') on possible fraudulent behaviour

Who are the data subjects? Who is (are) controller(s)? and/or processor(s)?

- a provider of modular HR cloud solutions uses a third party to provide a tool that enables its customers (employers) to calculate the (max) compensation they can pay employees for travel expenses
- business information bureaus such as Experian or Dun & Bradstreet generate credit scores and scorecards of companies and individuals, which customers use to assess the solvency of these companies and individuals.
- Cambridge Analytica processed personal data of US citizens
- what other example can you think of?

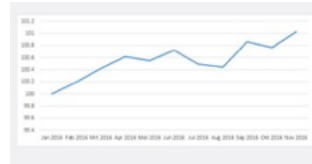
Who are the data subjects? Who is (are) controller(s)? and/or processor(s)?



The Raet Job Index refers to the jobs of employees who are employed by their employer and are active that month. The index does not include FTEs but the number of persons employed by an employer. Paid trainees and holiday workers are included. Temporary agency workers, volunteers, freelancers and unpaid trainees are not included.

The figures are based on transactional data about the number of actually paid employees of Raet's customers. The figures are therefore not dependent on the accuracy and completeness of surveys or polls. The figures are based on more than 1 million employees and extrapolated to the size of the Dutch labour force.

[translated with www.DeepL.com]



0.3% up in November
In November The Raet Jobs Index shows that the number of jobs of employees in the Netherlands increased in November 2016. The index stands at 101.0.

QUESTIONS

1. A company has a small ICT-department, consisting of five employees that provide ICT-support to other employees in the company. Does this ICT-department qualify as processor? Why (not)?

- A. Yes, because the five employees do process personal data on behalf of the company
- B. No, they are part of the organisation of the controller
- C. No, but the department could be a joint controller

Question 8 preparation assignment questions

SEMINAR I. AND II. 18 QUESTIONS

- In Seminar I professor Zwenne will discuss the history, content and background of European Data Protection Law: the legal framework and institutions. In Seminar II the key concepts applicability and territorial scope are relevant. For both seminars students are expected to have prepared answers on the questions below, which may be discussed in class.
1. When did the European Convention of Human Rights (ECHR) enter into force? What article of that Convention deals with privacy and data protection?
 2. Why did policymakers and lawmakers in some European countries use the need for data protection law (data privacy law) in the 1960s and the early 1970s?
 3. In 2016 the European Commission commented that "the diversity of national approaches and the lack of a system of protection at community level are an obstacle to completion of the internal market". How can this diversity be such obstacle?
 4. What is the role of the position papers, policy papers, and background papers by the EDPS? Are they highly binding?
 5. Which ECJ (EU) cases are considered particularly influential in shaping EU DP law?
 6. What are the definitions of the controller and the processor? Give a few real examples of both.
 7. What is meant by "joint controllership"? What are the consequences of such joint controllership?
 8. A company has a small ICT department, consisting of five employees that provide ICT-support to other employees in the company. Does this ICT-department qualify as processor? Why (not)?
 9. What was the SWIFT case about?
 10. Do pseudonymous data qualify as personal data? Why (not)?
 11. When is an individual considered to be identified or identifiable?
 12. Does EU DP law apply to manual (i.e. non-automated) processing of personal data?
 13. A data subject dies. Is his data still protected under EU DP law?
 14. What did the CJEU say about IP-addresses?
 15. What are "special data" or "special categories of personal data"?
 16. A controller decides to anonymise a personal data. Is the process of anonymisation covered by the concept of processing personal data?
 17. In the Google Spain case the Court ruled that the Spanish DP Act did apply to the processing of personal data controlled by Google Inc, which is established in Mountain View, CA in the US. How did the Court come to that decision?
 18. A Dutch electronics manufacturer instructs an India-based ICT service provider to analyse a set of personal data on individuals in South Africa, in order to sell its devices. Does the GDPR apply to personal data on individuals in South Africa, in order to sell its devices. Does the GDPR apply to

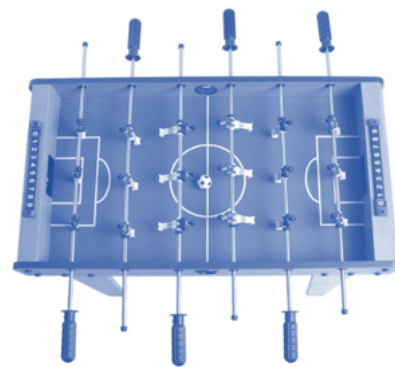
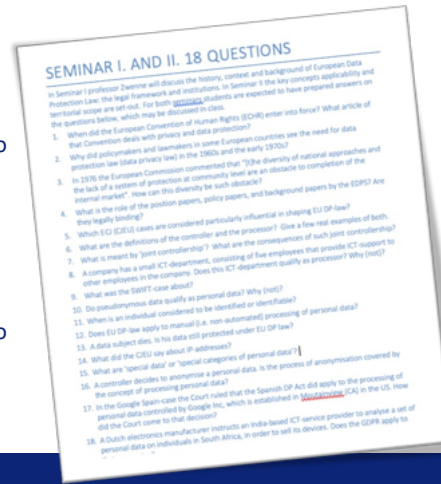


QUESTIONS

2. What was the SWIFT-case about?

- A. About an enormous data breach at the EMEA-headquarters of car manufacturer Toyota. In essence, the case was about the territorial scope of EU DP-rules
- B. This was about unauthorised data processing by the Society for Worldwide Interbank Financial Telecommunication, as a result of which SWIFT was deemed to be processor, acting on behalf of the banks
- C. This was about unauthorised data processing by the Society for Worldwide Interbank Financial Telecommunication, as a result of which SWIFT was deemed to be controller for that processing

Question 9 preparation assignment questions)



The playing field



"processing"

Art. 4(2) GDPR

any operation or set of operations,
which is performed upon personal data
or sets of personal data, whether or
not by automated means

*such as collection, recording, organization,
structuring, storage, adaptation or
alteration, retrieval, consultation, use,
disclosure by transmission, dissemination or
otherwise making available, alignment or
combination, erasure or destruction*

question

can you name an activity with respect to personal
data that is *not* covered by the definition of
'processing of personal data'



"personal data"

Art. 4(1) recital
26 GDPR

any information relating to an
identified or identifiable
natural person ("data subject")

*an identifiable person is one who can be identified,
directly or indirectly, in particular by reference to an
identifier such as a name, an identification number,
location data, unique identifier or to one or more
factors specific to the physical, physiological,
genetic, mental, economic, cultural or social or
gender identity of that person*

"anonymous data"

Art. 4(1) recital
26 GDPR

information that does not relate to an
identified or identifiable natural
person

*an identifiable person is one who can be identified, directly or
indirectly, in particular by reference to an identifier such as a
name, an identification number, location data, unique identifier
or to one or more factors specific to the physical, physiological,
genetic, mental, economic, cultural or social or gender identity
of that person*

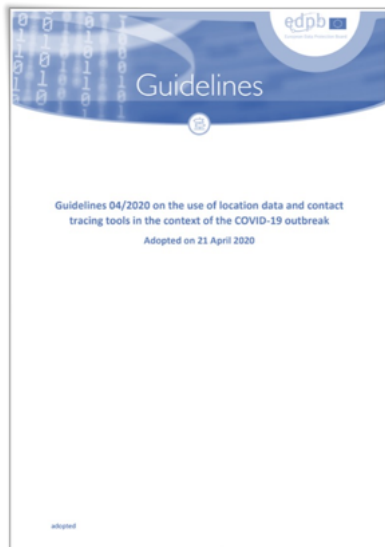


"pseudonymous data"

Art. 4(5) GDPR

personal data that cannot be attributed to a specific data subject without the use of additional information

as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution



Anonymisation refers to the use of a set of techniques in order to remove the ability to link the data with an identified or identifiable natural person against any "reasonable"

effort. This "reasonability test" must take into account both objective aspects (time, technical means) and contextual elements that may vary case by case (rarity of a phenomenon including population density, nature and volume of data). If the data fails to pass this test, then it has not been anonymised and therefore remains in the scope of the GDPR.



POLITICO



Meet the Dutchman who cried foul on Europe's tracking technology

The official privacy watchdog has the latest dispute with EU privacy watchdogs. His approach appears to be winning.

As European governments rushed to embrace technology to fight the coronavirus, a plainspoken Dutchman emerged as a thorn in their side. Aleid Wolfsen's message: Don't pretend your solutions are privacy-friendly.

In a group that normally keeps disagreements quiet, Wolfsen stands out. A former politician and mayor of Utrecht who had no formal training in data protection when he took on his role in 2016, he has repeatedly been at odds with her watchdogs, most of whom do not have a political background.



The official in charge of Europe's grouping of privacy regulators was also keen to play down any disagreements. There is "no difference in the positions" of different privacy regulators and the "Dutch case was a specific case," Andrea Jelinek said, while a spokesperson for the group, the European Data Protection Board, added: "The legal concept of anonymization is not an absolute concept."

Europe's Data Protection Supervisor, who had OK'd the Commission's use of telecoms data to track the coronavirus, said: "There is a difference between the technical impossibility of doing something to the very end, and something which we would call an effective anonymization."



info@companyname.com

social security number

@zwnne

ip-address
MAC-address

cookies, device fingerprints

zip code, street and/or house nr.

070 515 3000

+31(0)6 2251 8330

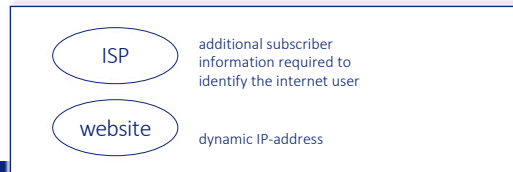


*“a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has **the legal means which enable it to identify the data subject** with additional data which the internet service provider has about that person”*

*CJEU 17 June 2021,
C-597/19 (Mircom)*

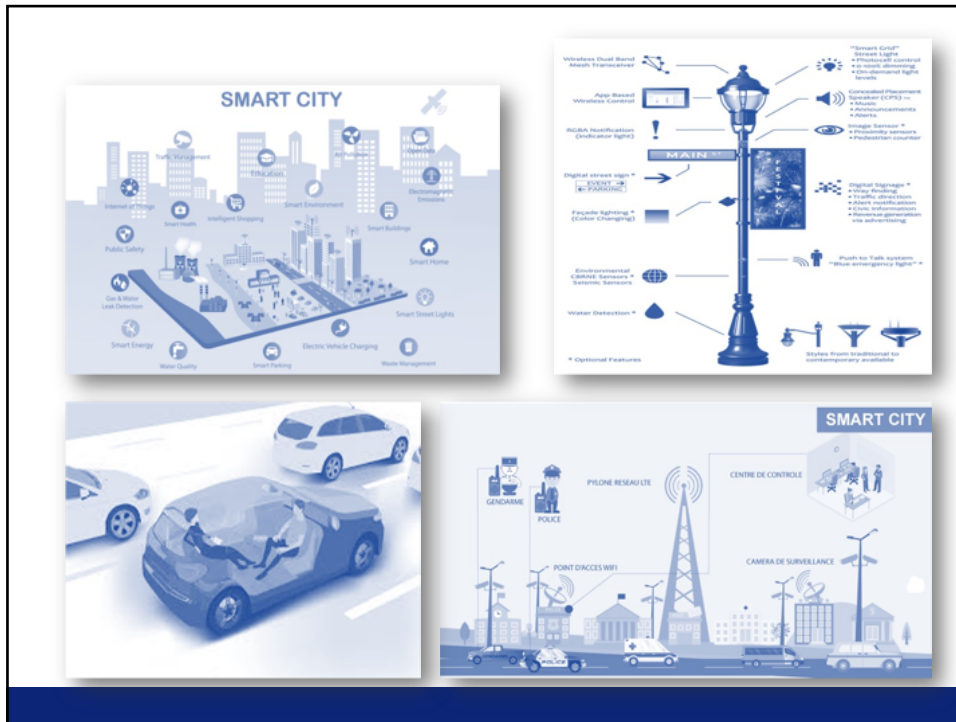


*CJEU 19 October
2016 C-582/14
(Breyer)*



- CJEU 19 October 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*)
- CJEU 20 december 2017, C-434/16 ECLI:EU:C:2017:99 (*Nowak*)
- CJEU 17 June 2021, ECLI:EU:C:2021:492 C-597/19 (*Mircom*)
- CJEU 26 April 2023, T-557/20, ECLI:EU:T:2023:219 (*GAR/EDPS*)
- CJEU 9 November 2023, C319/22- ECLI:EU:C:2023:837 (*Gesamtverband*)
- CJ EU 7 March 2024, C-604/22, ECLI:EU:C:2024:214 (*IAB*)





QUESTIONS

1. Do pseudonymous data qualify as personal data? Why (not)?

- A. No, because such data can no longer be attributed to a specific data subject without the use of additional information
- B. Yes, because such data could be attributed to a natural person by the use of additional information and consequently should be considered to be information on an identifiable natural person
- C. No, because such data is encrypted, implying that there are no means that are reasonably likely to be used to identify the natural person

Question 1a preparation assignment questions)



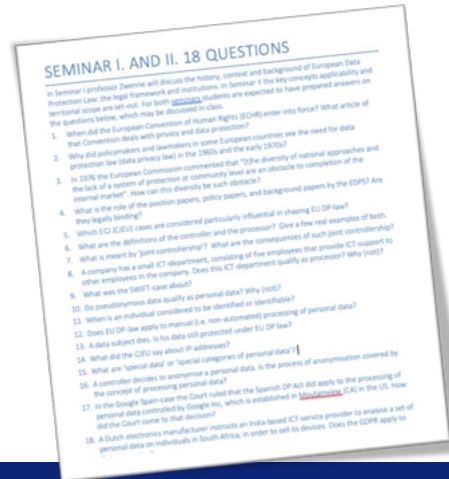


QUESTIONS

2. A data subject dies. Is his data still protected under EU DP law?

- A. Yes
- B. No
- C. Sometimes

Question 13 preparation assignment questions



material scope

DIRECTIVE (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties

main rule

GDPR applies to

- the processing of personal data wholly or partly by automated means
- sometimes also non-automated processing ("filing system")

any structured set of personal data which form part of a filing system or are intended to form part of a filing system

exceptions

- activities outside scope of EU law
- Ch. 2 Title V of Treaty on EU
- prevention investigation detection or prosecution of criminal offences
- processing for purely personal or household activity

processing of records of non-EU citizens, not in EU Member State, by non EU-based controller

common security and defence

*member state law to provide for exceptions for journalistic, artistic, or literary ends
Art. 85 GDPR*



*This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include **correspondence and the holding of addresses, or social networking** and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.*



Recital 18 GDPR

*the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which **also monitors a public space**, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.*



**CJEU 11 December
2014 C-212/13,
ECLI:EU:C:2014:2428
(Reynes)**



the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which **also monitors a public space**, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.



CJEU 11 December 2014 C-212/13, ECLI:EU:C:2014:2428 (Revnes)



What if the continuous recording device also monitors parts of another individuals space (e.g. a garden)

territorial scope under the GDPR

main rule

- processing in the context of the activities of an establishment of a controller or a processor in a Member State

sub rule (if no establishment in the EU)

- offering of goods or services to such data subjects in the union; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU



1. *who is the controller?*
2. *does the controller have an establishment in a Member State?*
3. *is processing taking place in the context of the activities of that establishment?*



territorial scope (Google Spain)

1. *who is the controller?*
2. *does the controller have an establishment in a Member State?*
3. *is processing taking place in the context of the activities of that establishment?*

*(55) In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment **if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.***

**AUTORITEIT
PERSOONSGEGEVENS**

Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition

03 September 2024 Themes: [Biometrics](#) [Personal data on the Internet](#)

The Dutch Data Protection Authority (Dutch DPA) imposes a fine of 30.5 million euro and orders subject to a penalty for non-compliance up to more than 5 million euro on Clearview AI. Clearview is an American company that offers facial recognition services. Among other things, Clearview has built an illegal database with billions of photos of faces, including of Dutch people. The Dutch DPA warns that using the services of Clearview is also prohibited.

Clearview is a commercial business that offers facial recognition services to intelligence and investigative services. Customers of Clearview provide camera images to find out the identity of people shown in the images. For this purpose, Clearview has a database with more than 30 billion photos of faces. Clearview scrapes these photos automatically from the Internet. And then it converts them into a unique biometric code per face. Without these people knowing and without them having given consent for this.

Clearview.ai

- *no establishment in the EU*
- *no services offered to data subjects in de EU*
- *data subjects monitored...?*

recital 24 GDPR

*In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are **tracked** on the internet including potential subsequent use of personal data processing techniques which consist of **profiling** a natural person, particularly in order to take decisions concerning her or him or for **analysing** or **predicting** her or his **personal preferences, behaviours and attitudes***

EDPB Guidelines 3/2016

- *behavioural advertisement*
- *geo-localisation activities, in particular for marketing purposes*
- *online tracking through the use of cookies or other tracking techniques such as fingerprinting*
- *personalised diet and health analytics services online*
- *CCTV*
- *market surveys and other behavioural studies based on individual profiles*
- *monitoring or regular reporting on an individual's health status*



- Koninklijke Philips N.V., a Dutch multinational tech company headquartered in Amsterdam (NL), intends to sell MRI-scanners and LED-lights in China. For that purpose Philips requests the data science department of the University of Mumbay (India) to analyse personal data of board members of Chinese health clinics.
- Cambridge Analytica Ltd based in London (UK) processed personal data of US citizens.
- As of 1st of January 2020, the successor of Cambridge Analytica processes personal data of Dutch citizens, living in Canada.
- An internet advertising network uses cookies to obtain data from internet-users, inter alia in the Netherlands

Is the GDPR applicable? Why (not)..?

Chicago Tribune

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.



QUESTIONS

1. A controller decides to anonymise a personal data. Is the process of anonymisation covered by the concept of processing personal data?

- A. Yes, anonymisation is processing
- B. No, anonymisation is not processing
- C. It depends, anonymisation can be processing, but not necessarily

Question 16 preparation assignment questions)

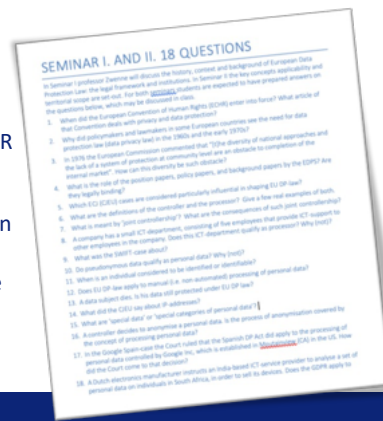


QUESTIONS

2. A Dutch electronics manufacturer instructs an India-based ICT-service provider to analyse a set of personal data on individuals in South Africa, in order to sell its devices. Does the GDPR apply to that processing?

- A. No, because no goods or service are offered to data subjects in the EU and/or there is no monitoring of their behaviour (as far as their behaviour takes place within the Union)
- B. No, the individuals are not in the EU, nor are the residents or citizens of member states, and consequently they are not protected by the GDPR
- C. Yes, as the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller in the Union, regardless of whether the processing takes place in the Union or not.

(Question 18 preparation assignment questions)





g.j.zwenne@law.leidenuniv.nl