Linguistics
Linguistique

ejtn

HANDBOOK

ON THE LANGUAGE OF DATA PROTECTION

With financial support from the Justice Programme of the European Union
Avec le soutien financier du Programme Justice de l'Union européenne

HANDBOOK

ON THE LANGUAGE OF DATA PROTECTION

With financial support from the Justice Programme of the European Union
Avec le soutien financier du Programme Justice de l'Union européenne

HANDBOOK ON THE LANGUAGE OF DATA PROTECTION.

European Judicial Training Network
Réseau européen de formation judiciaire

With financial support from the Justice Programme of the European Union
Avec le soutien financier du Programme Justice de l'Union européenne

ISBN-NUMBER: 9789464000924

FOREWORD OF THE EJTN'S SECRETARY GENERAL

Development of language skills is essential to enable exchanges between judicial authorities and individual judges, prosecutors and court staff, paving the way for mutual trust and a better understanding of foreign legal and judicial systems.[1] Thus, having a good command of a foreign language and its legal terminology should form an essential part of the training of the judiciary.

The European Judicial Training Network (EJTN) has devoted attention to the design and implementation of advanced and technical language trainings, in order to complement and support the basic language training primarily provided by its Members at national level. In 2019, over 600 participants are expected to attend the eleven linguistics trainings and four Summer Schools offered by EJTN's Linguistics Programme. EJTN's added value notably lies in the tools provided to all its Members such as linguistic handbooks and glossaries, self-assessment tests and marked tests available as e-learning modules.

This Handbook is one of such tools. It is the 1st edition of a linguistic handbook on data protection compiling the most relevant training materials used in EJTN linguistic courses delivered regularly in this area of law since October 2017.

The European Union data protection legislative package adopted in May 2016 aims at making Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU regardless of where their data is processed[2]. With this publication we aim to help members of the judiciary to be fit to contribute to achieving this goal by correct understanding and application of relevant EU law instruments. Definitions, exercises and examination of real cases make the Handbook an invaluable, hands-on resource.

On behalf of the EJTN, I would like to express my sincere gratitude to the authors of the texts and exercises in the Handbook for their dedicated work. I wish also to express appreciation to the EJTN Project Coordinator, Mr. Ondrej Strnad, for his dedication in carrying out the EJTN linguistic activities, as well as members of the EJTN Linguistic Sub-working Group, chaired by Ms. Renata Vystrčilová from the Czech Judicial Academy, which supervises all EJTN linguistic activities.

Enjoy using this Handbook.

Wojciech Postulski

EJTN Secretary General

1 EJTN Strategic plan for 2021-2027

2 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

LIST OF AUTHORS, EDITOR AND COORDINATOR

MOȚU, FLAVIUS IANCU

Judge at the Specialized Court of Cluj, Trainer for the National Institute of Magistracy, Romania.

PETRILÁKOVÁ, DENISA

Linguist and methodology consultant with the National Judicial Academy of the Slovak Republic, trainer and content designer with the National Judicial Academy of the Czech Republic. Legal English lecturer at the Supreme Court and the Supreme Administrative Court of the Czech Republic.

SAMANIEGO FERNÁNDEZ, EVA

Lecturer of ESP, Legal English and Legal Translation. Departamento de Filologías Extranjeras, UNED, Spain. Sworn legal translator. Teacher of Legal English for the Spanish Council of the Judiciary, ERA and EJN/Eurojust.

SIEROCKA, HALINA

Assistant Professor at the Faculty of Law, University of Bialystok in Poland; lawyer-linguist, the head of the Białystok Legal English Centre, a member of EULETA (the European Legal English Teachers' Association), an expert in legal discourse and translator.

WALBAUM ROBINSON, ISABEL ALICE

Lecturer of Legal English at the National School of the Judiciary, Naples, Italy. Retired from the University of Rome Three, School of Law (Università degli Studi di Roma Tre, Dipartimento di Giurisprudenza) as lecturer of English for Legal Studies.

Editor: ***ISABEL ALICE WALBAUM ROBINSON***

Coordinator: ***STRNAD, ONDREJ***

Project Manager, Linguistics Portfolio, Programmes Unit, European Judicial Training Network.

TABLE OF CONTENTS

UNIT 1. ____ 6

Introduction to EU Data Protection Law and the Language of Data Protection: Reading, Vocabulary and Language Practice.

UNIT 2. ____ 28

Data Protection Regulations and Directives: Vocabulary Building, Language Form and Language Practice.

UNIT 3. ____ 40

The Language of Data Protection: Cases and Fundamental Concepts.

ANSWER KEYS ____ 52

GLOSSARY ____ 59

SUMMARY OF CASES ____ 62

BIBLIOGRAPHY ____ 120

Unit 1

INTRODUCTION TO EU DATA PROTECTION LAW AND THE LANGUAGE OF DATA PROTECTION: READING, VOCABULARY AND LANGUAGE PRACTICE.

A. On Data Protection Law.

Flavius Iancu Motu

Why have we chosen to protect personal data in the EU?

"In ancient times, land was the most important asset, so politics was a struggle to control land. In the modern era, machines and factories became more important than land, so political struggles focused on controlling these vital means of production. In the twenty-first century, however, data will eclipse both land and machinery as the most important assets, and politics will be a struggle to control the flow of data. The race to obtain the data is already on, headed by data-giants such as Google and Facebook and, in China, Baidu and Tencent. So far, many of these giants seem to have adopted the business model of 'attention merchants'. They capture our attention by providing us with free information, services, and entertainment, and then they resell our attention to advertisers. Yet the data-giants probably aim far higher than any previous attention merchant. Their true business isn't to sell advertisements at all. Rather, by capturing our attention they manage to accumulate immense amounts of data about us, which are worth more than any advertising revenue. We aren't their customers—we are their product". [3]

What are 'personal data'?

Personal data are any data that allow our identification: name, personal identification number, image, fingerprints, DNA etc. Such data are intimately linked to every individual's unique personality and, therefore, their processing is protected as a fundamental right by Article 8 (1) of the Charter of Fundamental Rights of the European Union and by Article 16 (1) of the Treaty on the Functioning of the European Union. Protecting the processing of personal data goes beyond merely defending one's privacy: it prevents natural persons from becoming subjects of profiling and automated decisions, preserving their *relevance* as individuals in the ever-expanding global environment.

The comprehensive scope of this legal notion has generated a vast CJEU case law: from the classic features of a natural person, such as his/her name, to the dynamic IP of that person's computer, all the data that could lead to the identification of a natural person have been dubbed as 'personal data'.

3 Yuval Noah Harari, ***21 Lessons for the 21st Century***, (Jonathan Cape 2018) 77-78.

B. The Language of Legal English and EU Data Protection English.

Isabel Alice Walbaum Robinson

Languages define personal identities, but they are also part of a shared inheritance. They can serve as a bridge to other peoples and cultures by promoting mutual understanding and a shared sense of European identity.[4]

The *Handbook On the Language of Data Protection* is another step in the direction of the fulfilment of the objectives laid down by the Roadmap on the European Judicial Training Strategy 2019-2025[5]. One of the points highlighted by the Strategy specifies that "knowledge of foreign legal language is key to participation in cross-border activities and to smooth cross-border judicial proceedings and cooperation." The European Commission's multilingual policy for the learning of at least two additional languages other than the mother tongue is viewed as key to reaching the "united in diversity" objective.

The co-existence of 24 official European languages is a powerful instance of unity in diversity and a cornerstone of the European project.[6] Multilingualism is viewed as an added value for "languages unite people, render other countries and their cultures accessible and strengthen intercultural understanding." Moreover, "foreign language skills play a vital role in enhancing employability and mobility."[7] Without knowledge of at least one or preferably two additional languages, particularly in the legal profession, mutual trust in cross-border exchanges and enhanced cooperation would perhaps not have taken off as successfully as they have. The context in which the European Judicial Training Network (EJTN) activity is carried out reflects the interests and need of EU judiciaries to develop mutual trust and recognition of judgments in the spirit of fostering communication and the sharing of professional work.

Special features of Legal English

As a specific purposes language, legal English has, over the years, undergone numerous changes since the Norman invasion of Britain in 1066. The transformation of Old English from a prevalently Germanic language, at the sunrise of the Renaissance period, was considerable. For almost 300 years, "French was the language of legal proceedings" (Haig, R. 2015: 4). Modern English has been influenced by French and Latin in a significant way. In terms of "the use of Latin for written communication and record was […] due partly to the feeling that it was a language that had become fixed while the modern languages seemed to be variable, unregulated, and in a constant state of change." (Baugh A.C & Cable T. 2002: 153). The acquisition of large numbers of Latin and French words into the English language not only increased the English vocabulary but also enriched it, giving the language greater precision and a copious number of legal terms (Mellinkoff D. 1983). The author points out that the most intense period of borrowing from French into English took place between 1251 and 1400 (Mellinkoff D. 1983; in Jespersen 1955). According to Mellinkoff (1983), by 1500, as a result of the use of vocabulary from French and Latin, marking the end of the Middle English period, the language of the law featured a significant mix of Romance and Germanic borrowed vocabulary (*ibid*: 137). Speakers of the language were in the condition of "moving freely through Latin and French and other tongues, picking, discarding, uniting" (*ibid*: 137). The re-shaping of Modern and Post-Modern English, strongly influenced by borrowings from other languages, endowed the language of English

4 European Commission. Access: 20.11.19. Source: https://ec.europa.eu/education/policies/linguistic-diversity_en

5 Roadmap, European Judicial Training Strategy 2019-2025.

6 Accessed 21.11.19. Source: https://europa.eu/european-union/about-eu/eu-languages_en

7 Source: https://ec.europa.eu/education/policies/multilingualism/about-multilingualism-policy_en

law with a unique set of features, acquired over a span of three centuries, such as its rich vocabulary characterised by a large number of synonyms to denote the same concepts, and its resilience which permits speakers to move freely and with ease through Latin, French and other tongues (Melinkoff D. *ibid*: 137) even today. In regards to the language of the law, (Maley, Y. 2004: 11) states that "[l]anguage is medium, process and product in the various arenas of the law where legal texts, spoken or written, are generated in the service of regulating social behaviour", adding that "once norms and proceedings are […] institutionalised, a special legal language develops, representing a predictable process and pattern of functional specialisation."

Legal English and EU Data Protection English.

In this section we briefly illustrate some characteristics of legal English and EU law English by examining the terminology of the *acquis*.

Legal English and EU law English on the vocabulary of data protection may be classified into three distinct categories:

[1] *Single and multiword lexical units (MLU)* present in European Union primary and secondary legislation. Many of the terms are specifically defined (see Glossary section): 'biometric data', 'cross border processing', 'enterprise', 'filing system', 'genetic data', 'personal data', 'processing', 'recipient' and 'restriction of processing'.

[2] *Semi-technical terms* or legal homonyms[8] present in legal linguistics in reference to words whose denotation in legal contexts is unique, different from the meanings of the same terms used in general purpose language (Tiersma 1999). Some examples are: *action* meaning 'judicial proceeding', *aggravating circumstance(s)* meaning factor(s) that 'increase the level of culpability of an act resulting in harsher sentencing as consequence'; *covenant* meaning 'sealed contract'; *instrument* meaning 'legal document'; *party/parties* in civil cases meaning 'opponent(s) in legal dispute'; *instant case* meaning 'case at hand/case presently being dealt with'; *service/to serve* meaning 'to deliver a legal document'; *without prejudice* meaning 'without detriment to legal rights or legal claims'; *predispose* meaning 'to prepare for the commitment of a criminal action'; *precedent* meaning 'action that may be used as an example when dealing with similar actions at a later time' in general purpose language and 'judicial decision' in common law.

[3] *Legal terminology* shared by both legal English and EU data protection law English. Several, by no means exhaustive examples, are: *to abrogate* which means 'to repeal or pass legislation that goes against the prior law'; *to adduce* meaning 'to bring forward' as in 'add a sentence or part of it here'; *to adjudicate* meaning 'to deliver judgment'; *conveyance* or 'act of transfer of a legal property title'; *derogation* which means 'a partial abolishment of a law limiting its force', *injunction* meaning 'court prohibition ordering a party to halt a specific course of action'; *negligence* 'behaving without the care a person of ordinary prudence would exercise in a similar situation', *privacy by design* meaning 'building privacy and data protection into the design of information and communications systems and also technologies for compliance with privacy and principles of data protection'.[9]

8 Homonyms consist in one or two or even more words that are different in meaning even though they share the same spelling and sound.

9 Source: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Legal English and EU law English both include, as mentioned above, technical terms and expressions borrowed from other languages. Some representative examples are:

[1] *Latin terms in their original form:*[10] *acta juri imperii* meaning 'acts and omissions in the exercise of State authority';[11] *a fortiori* meaning 'for a more certain basis or reason'*;* *erga omnes* meaning 'towards all' as in 'rights and obligations for everyone'*;* *habeas corpus* meaning 'order of the court requesting a detained person to be brought before the judge'*;* *impetus* meaning 'force that drives a person to take action'*;* *inter alia* meaning 'among other matters or things'*,* *lex specialis* meaning 'doctrine that sets forth that where two laws exist in relation to the same facts, a law regulating a specific subject prevails over the general law'; *mutatis mutandi* meaning 'change where change is needed'**;** *ne bis in idem* meaning 'not a second time against the same legal action'**;** *prima facie* meaning 'enough at first view to ascertain a fact'; *proviso* meaning 'clause or stipulation as in a regulation in which a condition is introduced'; *res judicata* meaning 'a decided case'; *voi dire* or 'speak the truth' administered in the form of a declaration in court.

[2] *Integrated Latin origin terms* with a different meaning in law English than in general purpose English*: petition* or 'formal request to a court for a specific action' as in 'a petition to appeal'; *portability* (in the meaning of data portability) means the 'right of a person to receive personal data in a commonly used form in order to easily share it with another';[12] *prescription* meaning 'time limitation beyond which a debt or crime is no longer enforceable by law'; *action* meaning 'judicial proceeding' in legal English but 'to do something' in general purpose English; *avoid* meaning 'to cancel'; *without prejudice* meaning 'without loss of rights' in legal English but 'with no bias' in general purpose English (Mellinkoff D. *ibid:* 12).

[3] *Terms borrowed from other languages.* From French: *acquis communautaire* meaning 'body of European Union law'; *rapporteur* (Old French *raporteur*, from *reporter* meaning 'to bring back'); *consent* or 'to grant permission to' (Old French *consentir*; Latin *consentire*, equivalent of 'to accept', 'to allow'); *to defray* meaning 'to pay or bear costs' (Old French *defrayer,* equivalent to 'expense'); *tort* meaning 'damage caused by negligent act' (Old French: tort, 'fault'). From German through French: *warrant* 'to safeguard', 'to protect' (Old French *guarantir,* from Germanic *waren* meaning, 'to warn', 'to protect'. From Old Norse *ombudsman* which means 'person who investigates violations of citizens' rights with regards to the public sector including cases in which data protection rights against a citizen have not been respected or safeguarded'.

Legal English and EU data protection English also make use of two types of word combinations referred to as *collocations* and *binomials*. A collocation consists "in a non-lexicalized combination of two or more words that co-occur not by chance but regularly" (Walbaum Robinson, I.A. 2015)[13]. Collocations are distinguished from multiword lexical units in that they are not found in a dictionary or collection of terms of a language, except in collocation dictionary entries in which the range of combinations are made explicit. Binomials refer to word combination sequences made up of generally two to three lexical units belonging to

10 For the selection and analysis of terms to build the data protection corpus (i.e., large collection of documents of a related type on a specific subject matter), Wordsmith programme WS-Version 07 was used.

11 Source: Regulation EU) No 1215/2012, OJ L 351, 20.12.2012, Art. 1, par. 1.

12 Source: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

13 The process of lexicalization in linguistics means the incorporation of a term into the vocabulary of a given language.

the same word class (i.e., noun, verb, adjective, preposition), conjoined by additive (*and*), adversative (*but*) or alternative (*or*) conjunctions (Walbaum Robinson I.A. 2015). In the examples below you will recognize many of the word combinations found in regulations, directives, communications, opinions, recommendations and case law. Word combinations enrich the language and at the same time give the terminology greater precision and reduce ambiguity. You will find many examples of both in Units 1 to 3. Below is a non-exhaustive selection of collocations and binomials used in EU data protection law:

[1] *Collocations*:

(a) *Adjective + noun combinations:*

adopted provisions, automated decision-making, automatic storage, data protection, compulsory disclosure, enhanced cooperation,[14] historical research purposes, legal person, legitimate purposes, national provisions, natural person, personal data breach, personal processing, personal information, protection impact, protection rules, public interest, public security, referred decision, unauthorised disclosure.

(b) *Noun + verb combinations:*

articles referred, data processed, data transferred, decision referred, end-user concerned, individual concerned, questions referred, offences referred.

(c) *Noun + preposition* joined with *of, to*, *by*:

i. With *of*:

confidentiality *of* electronic communication; consent *of* the end-user; integrity *of* the information; interceptions *of* communication; principle *of* movement *of* personal data; proceeds *of* fraudulent activity; serious risk *of* circumvention.

ii. With *to*:

access *to* data; right *to* erasure; right *to* data portability.

iii. With *by*:

established *by* Decision 2000/520; imposed *by* competent national courts; imposed *by* supervisory authority; restricted *by* law; vested *by* the statute.

[2] *Binomials*.

(a) With *and:* clarifying *and* reinforcing; confidentiality *and* simplification; corrective powers *and* corrective sanctions; encrypted wireless networks *and* routers (i.e., networks of a certain type + routers); messaging services *and* web-based services; sanction *and* penalties; silent calls *and* nuisance calls; traffic *and* location (ref. to data); over *and* above as in 'Safe Harbour principles may take place without any additional condition over and above those for transfer to a third party'.

(b) With *but:* fundamental rights *but* awareness-raising as in 'Individuals make use of their fundamental rights *but* awareness raising should continue; conveyance of signals *but* also interpersonal communication services.

14 In some of these noun+noun combinations such as data protection and protection impact, the first noun functions as an adjective.

(c) With *or:* conclusion *or* performance as in 'The transfer is necessary for conclusion *or* performance of a contract concluded […]'; law *or* regulations as in 'the transfer is made from a register which according to law *or* regulations is intended to provide information […]'.

This short introduction to the *Handbook On the Language of Data Protection* brings to the fore several characteristics of both legal English and EU data protection law English. Terms, texts and topics exemplified are meant to be representative of the terminology you, as readers and professionals, encounter or will be encountering in your work environments. The activities included in the Handbook are meant to help you improve your reading and listening comprehension skills, to learn and practice using the key terminology, to focus on the meaning of words, to engage in discussions and debates, to exchange information with your colleagues, to write summaries, to provide answers to questions that make you reflect more on the readings, to increase your communicative competence by using your background knowledge of the law and also your professional experience.

Making a parallel between learning a language and learning the game of chess, Haig wrote "It is said of chess that the game takes a day to learn, and a lifetime to master" (Haig 2015: 5). Likewise, when it comes to learning English, we can also say that it is a rather easy language to learn at first try, but that it might take a lifetime of temporary or steady sojourn in an English-speaking country to obtain mother-tongue speaker fluency level.

While working with the Handbook, if some of the activities are too difficult to complete, I recommend consulting unknown words in a legal English dictionary. You will also find the official technical data protection terms in the Glossary. An alternative approach, to enhance meaning understanding, however, would be to try to figure out the meaning of the word(s) by assessing their grammatical features or the context surrounding the word. It is also useful to select the terms that you find most difficult or interesting and define them preferably in your own word(s). Only then consult the dictionary!

For an effective improvement of your listening competence, a skill that can be particularly difficult to master in a foreign language, I recommend first, to listen to the entire video without simultaneously completing the text (by gap filling); then, to listen to the video once more and add the missing words as you read along. Once the task is completed, take time to go over the text again and listen to the video one last time. In the Handbook you will also find activities that involve discriminating between or among technical terms, such as exercises involving term-definition matching or text-completion and many others.

Finally, it is our wish that this Handbook exemplifies the value placed on quality judiciary training for the purpose of sharing region-wide professional expertise and knowledge in the context of a rich and highly gratifying intercultural educational project developed and coordinated by EJTN and carried out with dedication and care by the EJTN group of linguistics and legal experts.

LANGUAGE EXERCISES

Exercise I.

The vocabulary of data protection.

Match terms with the corresponding definitions (1-20).

Data subject consent	Recovery	Data protection authority	Dissemination	Hacker
Judicial data	Remedy	Personal data filing system	Data processor	Firewall
Controller	Recipient	Processing of personal data	Security measures	Encryption
Personal data	Third party	Personal safety measures	Identifiable person	Privacy

1. _____: Any information concerning natural persons that are or can be identified also by way of other items of information - e.g., via a number or an ID code. For instance, personal data is one's first or last name, address, Tax ID as well as a picture, the recording of one's voice or one's fingerprint, or medical, accounting or financial information relating to that person;

2. _____: Person who can be spotted, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

3. _____: Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

4. _____: Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

5. _____: The competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law;

6. _____: Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

7. _____: Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

8. _____: An administrative independent authority set up by the national laws. Similar authorities have been set up in all EU countries pursuant to Article 8 of the Charter of Fundamental Rights of the European Union. The authority is tasked with ensuring the protection of fundamental rights and freedoms as regards the processing of personal data along with respect for individuals' dignity.

9. _____: Making personal data known to the public at large and/or to an indefinite amount of entities - for instance, by publishing personal data in a daily or posting personal data on a web page;

10. _____: The reduction of a readable file to coded language when an individual does not wish certain persons to see it;

11. _____: What is done to a file when one wishes to stop the file from being attacked by viruses;

12. _____: Persons who lawlessly utilize personal computers belonging to other individuals to steal data from them.

13. _____: Personal data disclosing that certain judicial measures have been taken in respect of a person such as to require their inclusion into that person's criminal record (e.g. final criminal convictions; paroling; residency and/or movement restrictions; measures other than custodial detention). The fact of being a defendant and/or the subject of criminal investigations falls within the scope of this definition as well;

14. _____: A natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not;

15. _____: Measures an individual takes to protect his/her data;

16. _____: Today it not only means the "right to be left alone" or to protect one's private sphere, as it is above all the right to be in control of how one's personal data are used and moved about. Personal information is actually the key commodity in today's information society;

17. _____: Judicial provision for any breach of the rights guaranteed to any person by national law applicable to the processing in question;

18. _____: Technical and organizational arrangements, electronic devices and/or computer software that are used to ensure that no data is lost or destroyed, even accidentally, only authorized entities may access the data, and no processing is performed either in breach of the law or by departing from that for which the data had been collected initially;

19. _____: What you do to your data when you want it back;

20. _____: The natural person, company, association or organization the Data Controller has entrusted with specific data processing management and control tasks on account of the relevant experience and/or skills.

Exercise II.

Working with prepositions.

Choose the correct option.

RIGHT OF ACCESS BY THE DATA SUBJECT.[15]

1. The data subject shall have the right (1) _____ obtain (2) _____ the controller confirmation as (3) _____ whether or not personal data concerning him or her are being processed, and, where that is the case, access (4) _____ the personal data and the following information:

(1)	a. of	b. for	c. to
(2)	a. from	b. of	c. off
(3)	a. for	b. to	c. of
(4)	a. to	b. at	c. towards

(a) the purposes **(5)** _____ the processing;

(5)	a. of	b. for	c. to

(b) the categories of personal data concerned;

(c) the recipient or categories of recipients (6) _____ whom the personal data have been or will be disclosed, in particular recipients (7) _____ third countries or international organisations;

(6)	a. at	b. for	c. to
(7)	a. in	b. at	c. on

(d) where possible, the envisaged period (8) _____ which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(8)	a. for	b. on	c. of

(e) the existence of the right to request (9) _____ the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object (10) _____ such processing;

(9)	a. from	b. of	c. off
(10)	a. to	b. at	c. through

15 Source: REGULATION (EU) 2016/679 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data.

(f) the right to lodge a complaint (11) _____ a supervisory authority;

(11)	a. to	b. at	c. with

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information (12) _____ the logic involved, as well as the significance and the envisaged consequences of such processing (13) _____ the data subject.

(12)	a. on	b. about	c. of
(13)	a. towards	b. for	c. to

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant (14) _____ Article 46 relating (15) _____ the transfer.

(14)	a. to	b. of	c. from
(15)	a. to	b. at	c. of

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested (16) _____ the data subject, the controller may charge a reasonable fee based (17) _____ administrative costs. Where the data subject makes the request (18) _____ electronic means, and unless otherwise requested by the data subject, the information shall be provided (19) _____ a commonly used electronic form.

(16)	a. by	b. from	c. of
(17)	a. at	b. upon	c. on
(18)	a. through	b. by	c. in
(19)	a. in	b. at	c. on

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect (20) _____ the rights and freedoms of others.

(20)	a. to	b. Ø	c. on

Exercise III.

Fundamental concepts of data protection.

The following linguistic exercises focus on practising the language related to the fundamental concepts of the Data Protection law.

TASK 1.

Please read and discuss the definition with your partner; (if using the handbook for self-study, try writing the definitions down and checking how well you did), go either to a Legal English Dictionary at https://www.translegal.com/legal-english-dictionary or to the following website of the European Data Protection Supervisor, search for the terminology and write down the definitions. https://edps.europa.eu/data-protection/data-protection/glossary_en)

To protect - protection

To process - processing of something

Data - personal data

To mean - the means

To process something by the means of equipment operated automatically

An individual - the individual data

To relate to something

A relative - to be related

Data related to an individual

To intend - an intention - intentionally

To file - a filing - a filing system

An access - accessible

A fall - to fall - to fall within

Person - personal

Personnel - personal

Personnel records - personal records

To hold - a holder

Court held - the records held

A set - to set something (to set up or set off)

A set of information

TASK 2.

Please go through Task 1 once again and find the words that match the following descriptions:

1. A submission submitted with a court
2. The devices or the instruments of achieving something
3. Deliberately
4. The way of getting to something
5. A person connected to one by family ties
6. Something related to a person
7. To be covered by a definition or a concept
8. The judge or a panel of judges decided
9. Employees, staff
10. An idea to do something deliberately to

TASK 3. Answers to key questions.

Answer questions 1-3 below.

1. Based on the above text, may a deceased persons' data be automatically and permanently protected?
2. Must the data (under UK law), in order to fall within the ambit of this definition, be in possession of the data controller?
3. Does the above text indicate that the data may only fall within the definition of personal protected data if an individual may be identified?

TASK 4. Fundamental terminology.

Read the extracts from legal provisions providing definitions of some fundamental data protection concepts and fill in the missing word (there is always just one word missing in the gap).

1. Data subject means an individual who is the subject (1) _____ personal data.
2. Data controller means a person who (either alone or jointly or) (2) _____ common with other persons) determines the purposes (3) _____ which and the manner in which any personal data are, or are to be, processed.
3. In relation to data controllers, the term (4) _____ is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently (5) _____ each other
4. Data processor, in relation to personal data, means any person (other (6) _____ an employee of the data controller) (7) _____ processes the data on behalf of the data controller.
5. Data processors are not directly subject (8) _____ the Act. However, most data processors, if not all, will be data controllers in (9) _____ own right for the processing they do for their own administrative purposes, such (10) _____ employee administration or sales.

TASK 5. Summarising.

Read the short example cases and write short summaries of those cases or record the summaries on your phone or Dictaphone. Then check the summaries you have written or recorded against the cases.

Case summaries to practice writing:

CASE 1:

An organisation holds data on microfiche. The microfiche records do not identify individuals by name but bear unique reference numbers which can be matched to a card index system to identify the individuals concerned.

Question for your partner (if working in pairs):

Is the information held on the microfiche records considered personal data?

The correct answer based on the above text is?

Yes, information held on the microfiche records is personal data.

CASE 2:

A government department sets up a database of information about every child in the country. It does this in partnership with local councils. Each council provides personal data about children in its area and is responsible for the accuracy of the data it provides. It may also access personal data provided by other councils (and must comply with the data protection principles when using that data).

Question for your partner (if working in pairs): Are the government department and the councils' data controllers in common in relation to the personal data on the database?

The correct answer based on the above text is?: Yes, the government department and the councils are data controllers in common in relation to the personal data on the database.

Case studies to practice speaking:

CASE 1:

A network of town-centre CCTV cameras is operated by a local council jointly with the police. Both are involved in deciding how the CCTV system is run and what the images it captures are used for.

Question for your partner: Are the council and the police joint data controllers in relation to personal data processed in operating the system?

The correct answer based on the above text is: Yes, the council and the police are joint data controllers in relation to personal data processed in operating the system.

CASE 2:

A utilities company engages a company which operates call centres to provide many of its customer services functions on its behalf. The call centre staff have access to the utilities company's customer records for the purpose of providing those services but may only use the information they contain for specific purposes and in accordance with strict contractual arrangements.

Question for your partner (if working in pairs): Does the utilities company remain the data controller or not? What is the position of the company that operates the call centre?

The correct answer based on the above text is: The utilities company remains the data controller. The company that operates the call centre is a data processor.

ADDITIONAL LANGUAGE PRACTICE

Exercise I. Word formation. Adjectives.[16]

Suffixation:

aggregate	**person**	**commerce**	**necessity**	**punish**
time	**consistence**	**analyze**	**analysis**	**identify**

Basic, no suffix to recognize:

core	**private**	**primary**	**ancillary**

Working with language form.

Complete the text with the appropriate adjectives.

The multinational's collection and use of **(1)** _____**ed** and **(2)** _____**al** data for advertising and other **(3)** _____**ial** purposes

Member States shall take the **(4)** _____**ry** measures to ensure that the offences referred to in Articles 3 to 7 as considered **(5)** _____**able** by a maximum term of imprisonment

The Chair shall have the task: a) to ensure the **(6)** _____**ly** performance of the tasks of the Board, in particular in relation to the **(7)** _____**ency** mechanism referred to in Article 63

The secretariat shall provide **(8)** _____**ical** support to the Board.

In the **(9)** _____ sector, the **(10)** _____ activities of a controller relate to its **(11)** _____**ary** activities and do not relate to the processing of personal data as **(12)** _____ **ary** activities.

The principles of protection must apply to any information concerning an **(13)** _____**ed** or **(14)** _____**able** person.

Article 27 may be a **(15)** _____**ful** instrument for providing guidance as to the ways in which data may be rendered **(16)** _____**ous.**

16 Examples for this exercise were selected from a corpus developed from a representative collection of EU data protection law documents (regulations, directives, recommendations, communications, opinions, case law …) with WordSmith Tools, WS-Version 7.0.

Exercise II. Reading and Vocabulary.

PART 1. Reading comprehension.

Go over the article and complete the exercises below.

Twin brothers sentenced for wire fraud, conspiring to hack into U.S. Department of State and private company. [17]

Two brothers, MA and SA, 23, of Springfield, Virginia, were sentenced today for conspiracy to commit wire fraud, conspiracy to access a protected computer without authorization and conspiracy to access a government computer without authorization. MA was also sentenced for accessing a protected computer without authorization, making a false statement and obstructing justice. MA was sentenced to 39 months in prison and SA was sentenced to 24 months in prison. Each man was also sentenced to three years of supervised release.

"The 'A' brothers misuse of their computer skills harmed numerous individuals and companies, and their efforts to gain clandestine access to State Department systems represented a threat to national security," said U.S. Attorney Dana J. Boente for the Eastern District of Virginia. "Electronic barriers are no less real, or legitimate, than physical ones. This prosecution sends a clear message to anyone else attempting to weaken the cybersecurity of institutions or use computers to commit crimes."

The brothers were indicted by a federal grand jury on April 30, 2015, and pleaded guilty on June 26, 2015. According to court documents, beginning in or about March 2014, MA hacked into the website of a cosmetics company and stole thousands of its customers' credit card and personal information. The 'A' brothers and co-conspirators used the stolen information to purchase goods and services, including flights, hotel reservations and attendance at professional conferences. MA also provided stolen information to an individual he met on the "dark net," who sold the information to other dark-net users and gave him a share of the profits.

In a separate scheme, the 'A' brothers and co-conspirators engaged in a series of computer intrusions and attempted computer intrusions against the U.S. Department of State to obtain sensitive passport and visa information and other related and valuable information about State Department computer systems. In or around February 2015, SA used his contract position at the State Department to access sensitive computer systems containing personally identifiable information belonging to dozens of co-workers, acquaintances, a former employer and a federal law enforcement agent investigating his crimes.

SA later devised a scheme to ensure that he could maintain perpetual access to desired State Department systems. SA, with the help of MA and co-conspirators, attempted to secretly install an electronic collection device inside a State Department building. Once installed, the device could have enabled SA and co-conspirators to remotely access and collect data from State Department computer systems. SA was forced to abandon the plan during its execution when he broke the device while attempting to install it behind a wall at a State Department facility in Washington, D.C.

Furthermore, beginning in or about November 2013, MA was performing contract work for a private data aggregation company located in Rockville, Maryland. He hacked into the company's database of federal contract information so that he and his brother could use the information to tailor successful bids to win contracts and clients for their own technology company. MA also inserted codes onto the victim company's servers that caused them to vote for Mr. 'A' in an online contest and send more than 10,000

17 Department of Justice. Office of Public Affairs Friday, October 2, 2015. Minor adaptations for educational purposes. Source: https://www.justice.gov/opa/pr/twin-brothers-sentenced-wire-fraud-conspiring-hack-us-department-state-and-private-company

mass emails to students at a local university, also for the purpose of garnering contest votes.

In or about October 2014, MA lied about his hacking activities and employment history on a government background investigation form while successfully obtaining a position with a defense contractor. Furthermore, in or about March 2015, after his arrest and release pending trial, MA obstructed justice by endeavoring to isolate a key co-conspirator from law enforcement officers investigating the conspirators' crimes. Among other acts, MA drove the co-conspirator to the airport and purchased a boarding pass, which the co-conspirator used to travel out of the country to the Republic of Malta. When the co-conspirator returned to the United States, MA continued to encourage the co-conspirator to avoid law enforcement agents.

[...]

PART 2. Text comprehension, key terms.

A. Are the following statements True or False?

1. Two brothers were taken into custody as suspects in a robbery. _____
2. Additional charges included access to unauthorized private computers. _____
3. The perpetrators were only given 39 and 24 months in jail. _____
4. According to the Department of Justice electronic barriers are as real as physical barriers are. _____
5. A federal Grand Jury charged[18] the two twin brothers. _____
6. The information obtained from the data was sold in the regular electronic information market. _____
7. Attempts to withdraw sensitive information from civil servants in the State Department were also made. _____
8. The perpetrators also tried to install a device into several State Department employees' personal computers that would allow them to withdraw information from the database on a regular basis. _____

B. What word/phrase is being described?

1. The act on behalf of the federal grand jury of accusing the A brothers. _____
2. The individual who penetrates a computer system for the sole purpose of destroying its security system. _____
3. The word used for the act of breaking into other people's computers and government databases without permission. _____
4. The word for content that exists and can be traded on the part of the web that is not indexed by search engines. _____
5. The word used to refer to persons one knows but are not friends such as coworkers and neighbors. _____
6. Those who enjoy and acquire advanced skills in computer programming, languages and codes for the purpose of exploring and discovering computer systems and networks. _____
7. One of the brothers committed the act of not revealing one of the principal co-conspirators. _____

18 formally accused.

C: Find a synonym for the words underlined.

1. […] Brothers MA and SA, "23, of Springfield, Virginia, were sentenced today for conspiracy to commit wire fraud". _____
2. "Each man was also sentenced to three years of probatory release". _____
3. MA also provided stolen information to an individual he met on the "dark net." _____
4. SA was forced to abandon the plan to place an electronic collection device to access computer systems during its execution when he broke the device while attempting to install it behind a wall at a State Department facility in Washington, D.C. _____
5. One of the brothers "hacked into the company's database of federal contract information so that he and his brother could use the information to tailor successful bids to win contracts and clients for their own technology company". _____

Exercise III. Reading and vocabulary building.

READING 1. EU Memo on data protection reform package.[19]

The task involves reading and working with three parts of speech: verbs, nouns and adjectives.

Introduction.

The data protection reform package which entered into force in May 2016 and will be applicable as of May 2018 includes the General Data Protection Regulation ("Regulation") and the Data Protection Directive for the police and criminal justice sector. The reform is an essential step to strengthening citizens' fundamental rights in the digital age and facilitating business by simplifying rules for companies in the Digital Single Market.

Working with near-synonyms.

Read the text and complete the sentences with the appropriate words based on the prompts provided.

What will change under the General Data Protection Regulation?

The Regulation updates and modernises the principles **(1)** _____ (*included*) in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on:

- reinforcing individuals' rights;
- strengthening the EU internal market;
- ensuring stronger enforcement of the rules;
- **(2)** _____ *(simplifying, improving)* international transfers of personal data and;

19 Source: http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm
Material to be used for educational purposes. Brussels, 24 May 2017. Accessed 21.10.2019.

- setting global data protection standards.

The changes will give people **more control** over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

What are the benefits for citizens?

The reform provides tools for **gaining control of one's personal data,** the protection of which is a fundamental right in the European Union. The data protection reform **will (3)** _____ (*give force to*) **citizens' rights and build trust.**

Nine out of ten Europeans have expressed concern about mobile apps collecting their data without their **(4)** _____ (*approval*), and seven out of ten worry about the potential use that companies may make of the information disclosed. The new rules address these concerns through:

1. **A "right to be forgotten"**: When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for **(5)** _____ _____ (*keeping*) it, the data will be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.

- **Easier access to one's data**: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A **right to data portability** will make it easier for individuals to transmit personal data between service providers.

- **The right to know when one's data has been hacked**: Companies and organisations must notify the national supervisory authority of data **(6)** _____ *(infractions)* which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures.

- **Data protection by design and by default**: 'Data protection by design' and 'Data protection by **(7)** _____ (*automatic setting*) are now essential elements in EU data protection rules. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

READING 2. The OLAF Data Protection Officer.[20]

Complete the gaps by adding the verbs in the appropriate tense.

Part 1. Working with verbs.

ensure **issue** **designate** **endorse** **set forth**

OLAF has **(1)** _____ *(designate)*, pursuant to Article 10(4) of Regulation (EU, Euratom) No 883/2013 and Article 24 of Regulation (EC) No 45/2001 Article 24 of Regulation (EC) No 45/2001, a Data Protection Officer (DPO). The new Regulation (EU)2018/1725 defines the role of the DPO in Articles 43-45.

The DPO **(2)** _____ *(ensure)* in an independent manner that OLAF correctly applies the rules protecting individual's personal data.

20 Source: https://ec.europa.eu/anti-fraud/olaf-and-you/data-protection/olaf-data-protection-officer_en Accessed 28.11.19. Adapted for educational purposes.

What does the Data Protection Officer do?

The tasks of the DPO are **(3)** _____ *(sets forth)* in Articles 44-45 of Regulation 2018/1725. Those tasks have been described in further detail by the EDPS Position Paper on the role of Data Protection Officers of the EU institutions and bodies, **(4)** _____ *(issue)* in September 2018. The DPO tasks are also set forth in the Decision of the Director General of OLAF of July 2019, adopting implementing rules concerning the Data Protection Officer pursuant to Article 45(3) of Regulation 2018/1725 and in the "Professional standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001", adopted by the network of EU DPOs in October 2010, and **(5)** _____ *(endorse)* by the European Data Protection Supervisor.

Part 2. Working with data protection vocabulary.[21]

Fill the gaps using the clues given in parenthesis with adjectives . In some instances you will be adding the adjective from the noun. Source: Regulation (EU) 2018/1725.

Article 44

Position of the data protection officer

1. The Union institutions and bodies shall ensure that the data protection officer is involved, properly and in a **(1)** _____ (*well-timed*) manner, in all issues which relate to the protection of personal data.

2. The Union institutions and bodies shall support the data protection officer in performing the tasks referred to in Article 45 by providing resources necessary to carry out those tasks and access to personal data and **(2)** _____ (*running*) operations, and to maintain his or her **(3)** _____ (*highly skilled in specific sector*) knowledge.

3. The Union institutions and bodies shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the **(4)** _____ *(maximum, top)* management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer and his or her staff shall be bound by **(5)** _____ *(something not revealed, concealed)* or confidentiality concerning the performance of their tasks, in accordance with Union law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

7. The data protection officer may be consulted by the controller and the processor, by the staff committee concerned and by any individual on any matter concerning the interpretation or application of this Regulation, without them going through the **(6)** _____ (*authoritative*) channels. No one shall **(7)** _____ (*endure, be the victim of*) prejudice on account of a matter brought to the attention of the **(8)** _____ (*qualified*) data protection officer alleging that a breach of the provisions of this Regulation has taken place.

21 Full source: Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002/EC. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

8. The data protection officer shall be designated for a term of three to five years and shall be **(9)** _____ (*entitled*) for reappointment. The data protection officer may be dismissed from the post by the Union institution or body which designated him or her if he or she no longer fulfils the conditions required for the performance of his or her duties and only with the consent of the European Data Protection Supervisor.

9. After his or her designation the data protection officer shall be registered with the European Data Protection Supervisor by the Union institution or **(10)** _____ (*entity)* which designated him or her.

Part 3. Working with nouns.

Fill the gaps using the clues given in parenthesis with adjectives. In some instances you will be adding the adjective from the noun.

Article 45

Tasks of the data protection officer

1. The data protection officer shall have the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union data protection (1) **p**_____ *(measures)*;

(b) to ensure in an independent manner the internal application of this Regulation; to monitor (2) **c**_____ (*respect for prescribed rules*) with this Regulation, with other applicable Union law containing data protection provisions and with the (3) **p**_____ (*action plans)* of the controller or (4) **p**_____ (*processing unit person*) in relation to the protection of personal data, including the assignment of responsibilities, the raising of (5) **a**_____ (*cognizance*) and training of staff involved in processing operations, and the related (6) **a**_____ *(control of financial accounts)*;

(c) to ensure that data subjects are informed of their rights and obligations pursuant to this Regulation;

(d) to provide advice where requested as regards the necessity for a notification or a (7) **c**_____ (*kind of information transmission*) of a personal data breach pursuant to Articles 34 and 35;

(e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 and to consult the European Data Protection Supervisor in case of (8) **d**_____ (*skepticism*) as to the need for a data protection impact assessment;

(f) to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior (9) **c**_____ (*consideration of advice*);

(g) to respond to requests from the European Data Protection Supervisor; within the sphere of his or her (10) **c**_____ *(ability, qualification)*, to cooperate and consult with the European Data Protection Supervisor at the latter's request or on his or her own initiative;

(h) to ensure that the rights and freedoms of data subjects are not adversely affected by processing operations.

2. The data protection officer may make recommendations to the controller and the processor for the practical improvement of data protection and advise them on matters concerning the application of data protection provisions. Furthermore, he or she may, on his or her own initiative or at the request of the controller or the processor, the **(11) s**_____ (*personnel*) committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice, and report back to the person who commissioned the investigation or to the controller or the processor.

3. Further implementing rules concerning the data protection officer shall be adopted by each Union institution or body. The implementing rules shall in particular **(12) c**_____ (*involve*) the tasks, duties and powers of the data protection officer.

Part 4. Reading. The relation between DPO – EDPS. [22]

Go over the text, complete the exercises and write down or share the answers to questions (1-6).

In order to ensure effective internal application of the Regulation, the working relationship between the DPO and the EDPS is of high importance. The DPO must not be seen as an 'agent' of the EDPS, but as a part of the EUI where they work. As already mentioned, this idea of proximity puts them in an ideal situation to ensure compliance from the inside and to advise or to intervene at an early stage, thereby avoiding possible intervention from the supervisory authority. At the same time the EDPS can offer valuable support to DPOs in the performance of their function.

The EDPS therefore supports the idea of further developing collaboration between DPOs and the EDPS, which contribute to achieving the overall aim of effective protection of personal data within the EUIs.

6.1. Ensuring application

Ensuring application notably starts by raising awareness. As mentioned above, the DPO plays an important role in developing knowledge on data protection issues inside the EUI. The EDPS welcomes this and the consequence in terms of stimulating an efficient preventive approach rather than repressive data protection supervision.

The DPO also provides advice to the EUI on practical recommendations for improvement of data protection within the EUI, or concerning the interpretation or application of the Regulation. This advisory function is shared with the EDPS who shall advise all EUIs on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data. In this field, the EDPS has often been called upon to advise DPOs on specific issues related to data protection (informal consultations). The EDPS also intends to revise existing positions papers and guidelines and issue new ones where required in order to continue providing guidance to the EUIs on a wide range of topics.

Part 5. Working with single words, word combinations and binomials[23].

Complete the text by adding the appropriate terms. Use the prompts to complete the exercise.

6.2. Enforcement

In the area of implementation of particular data protection measures, **(1)** _____ (*cooperation interaction*) potentials between the DPOs and EDPS emerge as regards the adoption of sanctions and handling of complaints and queries. As already mentioned, the DPOs have **(2)** _____ _____ (*reduced potential*) of enforcement. The EDPS will contribute to ensuring compliance with the Regulation by taking

22 Source: European Data Protection Officer, Position Paper on the Role of Data Protection Officers of the EU Institutions and Bodies. Published 2019, pps 15-16.

23 'Binomial' is the term used in linguistics to mean the combination of two words linked by conjunctions *and, but, or.*

effective measures in the field of prior consultations, complaints and other inquiries. Measures are effective if they are well-targeted and feasible and the DPO can also be seen as a strategic partner in determining the well-targeted application of a measure.

As mentioned above, the handling of **(3)** _____ and _____ (*expressions of dissatisfaction + doubts*) by the DPO at a local level is to be encouraged, at least as concerns a first phase of **(4)** _____and _____ *(inquiry + problem resolving)*. The EDPS therefore believes that DPOs should try to investigate and resolve complaints within the EUI before referring to the EDPS. The DPO should also be invited to consult the EDPS whenever they have doubts on the procedure or substance of complaints. The limited powers of enforcement of the DPO may also lead them to escalate certain matters to the EDPS for support. Such consultations can naturally be made without involving the EUI. In certain sensitive cases where the DPO **5)** _____ *(being afraid of)* repercussions from their EUI if they act upon a complaint, it may be preferable for the EDPS to handle the complaint or open an **(6)** _____-_____ *(personally driven decision)* inquiry.

This does not, however, prevent the data subject from lodging a complaint directly with the EDPS under Article 57(1)(e). The EDPS therefore provides valuable support in the field of enforcement. In turn, the DPO can be relied upon to provide information to the EDPS and to provide follow-up on the measures adopted. The DPO is in copy of all communication with the EUI in the **(7)** _____ (*structure that lies under*) of complaints and is thus kept informed of the investigation and its outcome.

6.3. Measuring effectiveness

As concerns measuring the effectiveness of the implementation of the data protection requirements, the DPO should be seen as a **(8)** _____ _____ (*important associate*) to evaluate progress in this area. For example, when it comes to measuring performance of internal data protection supervision, the EDPS encourages DPOs to develop their own criteria of good supervision, professional standards, specific plans for the institution, annual work programme, etc.). These criteria will in turn enable the EDPS, where invited to do so, to evaluate the work of the DPO, but will also allow them to measure the state of implementation of the Regulation within the EUI.

Part 6. Questions.

Write down the answers to questions 1-6, preferably in 'your own words'.

1. *Which are the conditions for an effective relationship between DPO and EDPS?*
2. *Why is it so important to avoid a repressive data protection supervision as opposed to a preventive one?*
3. *What actions are involved for a DPO in his/her advice provider role?*
4. *Which actions could be considered an example of a:*
    a. *preventive approach to data protection?*
    b. *repressive approach to data protection?*
5. *What is meant by a 'natural person?*
6. *In a nutshell, which are the responsibilities of the DPO?*

Unit 2

DATA PROTECTION REGULATIONS AND DIRECTIVES: VOCABULARY BUILDING, LANGUAGE FORM AND LANGUAGE PRACTICE.

INTRODUCTION

Flavius Iancu Motu

Which are the legal instruments that protect personal data?

Following the harmonizing objectives and principles of Directive 95/46/EC, Regulation 2016/679 of the European Parliament and of the Council (GDPR), having direct effect in all EU Member States, provides a comprehensive list of definitions covering the essential legal terminology of personal data protection along with the principles of personal data processing and the rights of the data subject and their restrictions. The GDPR also regulates the activities of the controller and of the processor and introduces a new actor, the data protection officer, along with providing mechanisms for demonstration of compliance with the principles and rules of personal data protection. Finally, the GDPR sets up the rules applicable to the international transfers of personal data and a consistency mechanism, under the authority of the European Data Protection Board, enabling the data subjects with effective remedies for the situation of an infringement of their rights.

Created as a carve-out of the GDPR, Directive (EU) 2016/680/EU regulates 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. Following the same principles of personal data processing, Directive (EU) 2016/680 lays down the data subject rights in the context of the enforcement of criminal law along with the prerogatives of the public authorities and their limits.

Finally, Directive 58/2002/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications - not yet in force - outline the features specific to the protection of personal data in the ever changing electronic environment.

LANGUAGE EXERCISES

Exercise I: The vocabulary of data protection regulations and directives.

TASK 1. Vocabulary building.

Read the excerpt from REGULATION (EU) 2016/679 and complete the extracts with the appropriate form of the capitalised words.

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, FAIR and TRANSPARENTLY);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is COMPATIBILITY with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data MINIMISE');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are ACCURACY, having regard to the purposes for which they are processed, are erased or rectified without LATE ('accuracy');

(e) kept in a form which permits identification of data subjects for no LENGTH than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) SUBJECTIVE to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against AUTHORISE or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and CONFIDE').

2. The controller shall be responsible for, and be able to demonstrate COMPLY with, paragraph 1 ('accountability').

TASK 2. Prepositions.

Complete the excerpt from REGULATION (EU) 2016/679 with the appropriate preposition.

at	**in**	**into**	**out**
to	**to**	**to**	**with**

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and **(1)** _____ the extent that at least one of the following applies:

   (a) the data subject has given consent **(2)** _____ the processing of his or her personal data for one or more specific purposes;

   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps **(3)** _____ the request of the data subject prior to entering **(4)** _____ a contract;

   (c) processing is necessary for compliance **(5)** _____ a legal obligation to which the controller is subject;

   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

   (e) processing is necessary for the performance of a task carried **(6)** _____ in the public interest or in the exercise of official authority vested in the controller;

   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, **(7)** _____ particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply **(8)** _____ processing carried out by public authorities in the performance of their tasks.

TASK 3. Working with word forms.

Read the excerpt from DIRECTIVE (EU) 2016/680 and choose the correct part of speech (adjective, adverb) for each of the gaps in the text.

Article 4

Principles relating to processing of personal data.

Select the appropriate term for (a) – (f).

1. Member States shall provide for personal data to be:

   (a) processed **lawful / lawfully** and **fair / fairly**;

   (b) collected for specified, **explicit / explicitly** and legitimate purposes and not processed in a manner that is **incompatible / incompatibly** with those purposes;

   (c) **adequate / adequately**, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are **inaccurate / inaccurately**, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures **appropriate / appropriately** security of the personal data, including protection against unauthorised or unlawful processing and against **accidental / accidently** loss, destruction or damage, using appropriate technical or organisational measures.

TASK 4. Formal legal English vocabulary.

Read the extract from DIRECTIVE (EU) 2016/680 and find more formal equivalents for the words in bold.

Any processing of personal data must be lawful, fair and **a) t**_____ **(clear / open)** in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as **b) c**_____ **(secret / covered)** investigations or video **c) s**_____ **(observation)**. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of **d) t**_____ **(harms / pains)** to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with **e) d**_____ **(suitable)** regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct **f) n**_____ **(concept / idea)** from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be **g) e**_____ **(clearly expressed)** and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for **h) e**_____ **(deleting / correcting)** or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

TASK 5. Key terms.

Match the words in Columns A and B. Use the words to complete the gaps from the extract of Directive 2002/58/EC.

Column A	**Column B**
(a) Direct	(1) intervention
(b) Electronic	(2) legislation
(c) Human	(3) mail
(d) National	(4) marketing
(e) Communications	(5) unsolicited

1. The use of automated calling systems without **(1)** _____ (*automatic calling machines*), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. (…)

4. In any event, the practice of sending **(2)** _____ for purposes of **(3)** _____ disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable **(4)** _____, that the legitimate interests of subscribers other than natural persons with regard to **(5)** _____ are sufficiently protected.

TASK 6. Corresponding terms.

Read the excerpt from Directive 2002/58/EC and find the corresponding words for the paraphrases or near-synonyms given below.

Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 10

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls

[1] to keep safe from danger, attack, or harm (v.) -

[2] in an association with (expression) -

[3] a violation (n.) -

[4] to modify / counteract (v.) -

[5] vicious / spiteful (adj.) -

[6] a refusal (n.) -

TASK 7. Working with definitions.

Read the excerpt from REGULATION (EU) 2016/679 and correct the definitions which are mixed up (not in the correct order).

1. **'genetic data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

2. **'profiling'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

3. **'processor'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

4. **'pseudonymisation'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

5. **'personal data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

6. **'biometric data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

7. **'filing system'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

8. **'recipient'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. **'processing'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

10. **'consent'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

11. **'controller'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Exercise II. The language of Regulation (EU) 2018/1725.

Fill in the blanks with the correct form or tense of the words in brackets.[24]

A **(1)** _____ [*datum*] subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at **(2)** _____ [*reason*] intervals, in order to be aware of, and **(3)** _____ [*verification*], the **(4)** _____ [*law abiding*] of the processing. This includes the right for data subjects to have access to data **(5)** _____ [*concern*] their health, for example the data in their medical records containing information such as diagnoses, **(6)** _____ [*exam*] results, assessments by treating physicians and any treatment or interventions **(7)** _____ [*provision*]. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data **(8)** _____ _____ [*process*], where possible the period for which the personal data are processed, the recipients of the personal data, the **(9)** _____ [*logical*] involved in any automatic personal data processing and, at least when based on **(10)** _____ [*profile*], the consequences of such processing. That right should not **(11)** _____ [*adversary*] affect the rights or freedoms of others, including trade secrets or **(12)** _____ [*intellect*] property and in particular the copyright protecting the software. However, the result of those considerations should not be a **(13)** _____ [*refuse*] to provide all information to the data subject. Where the controller processes a large **(14)** _____ [*quantify*] of information concerning the data subject, the controller should be able to request that, before the information **(15)** _____ [*delivery*], the data subject specify the information or processing activities to which the request relates.

A data subject should have the right to have personal data **(16)** _____ [*concern*] him or her rectified and a 'right to be forgotten' where the **(17)** _____ [*retain*] of such data infringes this Regulation or Union law to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer **(18)** _____ [*need*] in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is **(19)** _____ [*relevance*] in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal

24 Source: Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be **(20)** _____ [*law*] where it is necessary, for exercising the right of **(21)** _____ [*free*] of expression and information, for **(22)** _____ [*compliant*] with a legal obligation, for the **(23)** _____ [*perform*] of a task carried out in the public interest or in the exercise of official **(24)** _____ [*authorise*] vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or **(25)** _____ [*history*] research purposes or **(26)** _____ [*statistics*] purposes, or for the establishment, exercise or **(27)** _____ [*defend*] of legal claims.

ADDITIONAL LANGUAGE EXERCISES

Exercise I. Often misused words.

Fill the spaces with the appropriate words. In this exercise attention should be given to the meaning of each single word in the context of the whole sentence. Some words, as in the case of many in the English language, are the same in form but diverse in meaning. Pay attention to the form of the terms and make the necessary adjustments for grammar where necessary. In two sets of confusing terms (save/save; sanction/sanction) you need to make choices based on the words in parenthesis.

1. **Acquire/Acquiesce**
   a. The participants have _____ knowledge of many legal English technical terms.
   b. The defendant _____ to the requests indicated by the court.
2. **Resume/Adjourn**
   a. It looks like the afternoon session is about to _____.
   b. The court decided to _____ to next Thursday.
3. **Advice/Advise**
   1. My colleague gave me some common sense _____.
   2. I _____ you to make sure your new habitual residence is registered.
4. **Sanction (*allow*)/Sanction (*prohibit*)**
   a. The State is planning to _____. all vehicles with high carbon emissions.
   b. After much debate, same-sex marriages are _____. in most European countries.
5. **Proceedings/Procedure**
   a. The judge stayed the _____ due to insufficient documentation.
   b. The _____ was long and tortuous. There appeared to be no possibility for a settlement on behalf of the parties.

6. **Remember/Remind**

   a. Could you _____ me to set the alarm before going to bed this evening?

   b. Did you _____ to lock the door before leaving the apartment?

7. **Specially/Especially**

   a. Council Regulation (EU) 206/1103 is _____ designed for dealing with EU cases related to the recognition and enforcement in matters of matrimonial property.

   b. The estranged couple were _____ adamant about custody of their two children.

8. **Save (*except for*)/Save (*help*)**

   a. The EU _____ many persons every year by taking proactive rather than post active measures with regards to data protection matters.

   b. A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' should be granted _____ exceptions provided by the law

Exercise II. Collocations and expressions in the language of data protection.

The following word combinations, known as collocations[25], are frequent in EU law as well as in the sector of data protection. *Provide the missing word to complete the collocation. A prompt has been provided for each collocate:*

1. Personal _____ (*information*).
2. Injured _____ (*victim of data protection violation*).
3. Right _____ (*to have information eliminated from web*).
4. (*violation*) _____ procedure.
5. (*relevant*) _____ law.
6. Appropriate _____ (*taking care of problems/situations*).
7. (*regular, consistent checks*) _____ monitoring.
8. (adj. *having legal validity/applicability*) _____ judgment.
9. Appropriate _____ (*care to avoid damage*).
10. Authentic _____ (*tools*).
11. Data _____ (*capacity to be transported*).
12. DPO _____ (*neutral, not aligned stance*).

25 Collocations are combinations of single words. Together, collocations enrich the meanings of each of the components, add new meaning and precision while reducing ambiguity.

Exercise III. Reading activity. Communication on the data protection framework.

Task 1.

Read the excerpt from Communication from the Commission to the European Parliament and the Council Data protection rules as a trust-enabler in the EU and beyond – taking stock COM (2019) 374 ***and choose the best answer a, b, c or d.***

(1)	a) expression	b) pronouncement	c) statement	d) verbalisation
(2)	a) cancel	b) obviate	c) reaffirm	d) repeal
(3)	a) adapting	b) adopting	c) conforming	d) transforming
(4)	a) exertion	b) application	c) fulfilment	d) utilisation
(5)	a) sorrows	b) grievances	c) loads	d) burdens

One continent, one law: the data protection framework is in place in Member States

One key objective of the Regulation was to do away with a fragmented landscape of 28 different national laws that existed under the previous Data Protection Directive[26] and to provide legal certainty for individuals and businesses throughout the EU. That objective has been largely met.

The harmonisation of the legal framework

Although the Regulation is directly applicable in the Member States, it obliged them to take a number of legal steps at national level, in particular to set up and allocate powers to the national data protection authorities[27], lay down rules on specific issues, such as the reconciliation of the protection of personal data with freedom of **(1)** _____ and information, and amend or **(2)** _____ sectoral legislation with data protection aspects. At the time of this Communication, all but three[28] Member States had updated their national data protection law. Work on **(3)** _____ sectoral laws is still on-going at national level. Following its incorporation in the European Economic Area Agreement, the application of the Regulation was extended to Norway, Iceland and Lichtenstein which have also adopted their national data protection law.

However, stakeholders are calling for an even higher degree of harmonisation in some areas[29]. Indeed, the Regulation allows Member States some scope to further specify its **(4)** _____ in certain areas such as the age of consent by children for online services[30] or the processing of personal data in areas such as medicine and public health. In this case, the action of Member States is framed by two elements:

i) any national specification law must meet the requirements of the Charter of Fundamental Rights[31] (and not go beyond the limits set by the Regulation which builds on the Charter);

ii) it may not impinge on the free flow of personal data within the EU[32].

In some instances, Member States have introduced national requirements on top of the Regulation, in

26 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

27 Such as the power to impose administrative fines.

28 As of 23 July 2019, Greece, Portugal and Slovenia are still in the process of adopting their national law.

29 See report of the Multi-stakeholder Group on the Regulation issued on 13 June 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

30 13 years for Belgium, Denmark, Estonia, Finland, Latvia, Malta, Sweden and the United Kingdom; 14 years for Austria, Bulgaria, Cyprus, Spain, Italy and Lithuania; 15 years for Czechia and France; 16 years for Germany, Hungary, Croatia, Ireland, Luxembourg, the Netherlands, Poland, Romania and Slovakia.

31 Article 8.

32 In line with Article 16(2) of the Treaty on the Functioning of the European Union.

particular through many sectoral laws and this leads to fragmentation and results in creating unnecessary **(5)** _____. One example of an additional requirement introduced by Member States on top of the Regulation is the obligation under the German legislation to designate a Data Protection Officer in companies with 20 employees or more permanently involved in automated processing of personal data.

Task 2.

Read the excerpt from Communication from the Commission to the European Parliament and the Council Data protection rules as a trust-enabler in the EU and beyond – taking stock COM (2019) 374 ***and complete the gaps with missing words. The first letter is given to help you.***

Continuing efforts towards greater harmonisation

The Commission engages in bilateral dialogues with national authorities, where it pays particular **(1) a**_____ to the national measures in relation to:

- the effective independence of data protection authorities, including through adequate financial, human and technical resources;
- how national laws **(2) r**_____ the rights of data subjects;
- the fact that **(3) n**_____ legislation should not introduce requirements going beyond the Regulation when there is no margin for specification, such as additional conditions for processing;
- fulfilling the **(4) o**_____ to reconcile the right to the protection of personal data with freedom of expression and information, taking into account that this obligation should not be misused to creating a chilling effect on journalistic work.

The work of the data protection authorities, cooperating in the context of the European Data Protection Board ('the Board'), is a key driver to a consistent **(5) a**_____ of the new rules: **(6) e**_____ actions affecting several Member States go through the cooperation and consistency mechanism[33] within the Board and the guidelines adopted by the Board contribute to a harmonised understanding of the Regulation. There is nevertheless an expectation on the part of stakeholders for the data protection authorities to go further in this direction.

The work of national **(7) c**_____ and the Court of Justice of the European Union is also helping to create consistent **(8) i**_____ of data protection rules. National courts have recently issued judgements invalidating provisions in national laws which depart from the Regulation[34].

33 Article 60 of the Regulation provides for cooperation between data protection authorities to apply one interpretation of the Regulation in concrete cases. Article 64 provides that the Board will issue opinions in certain instances so as to ensure consistent application of the Regulation. Finally, the board is given the power to adopt binding decisions addressed to the data protection authorities in case of disagreement between them.

34 This has been the case in Germany and in Spain.

Exercise IV. Acronyms and abbreviations[35].

Test your background knowledge by completing the abbreviations using the tips provided.

1. CCTV (C _ _ _ _ _ C _ _ _ _ _ _ Television)

2. CIS (C _ _ _ _ _ s I _ _ _ _ _ _ _ _ _ n System)

3. EDPS (E _ _ _ _ _ _ n D _ _ _ P _ _ _ _ _ _ _ _ n S _ _ _ _ _ _ _ _ r)

4. C-SIS (C _ _ _ _ _ l - S_ _ _ _ _ _ n I _ _ _ _ _ _ _ _ _ n S_ _ _ _ m)

5. DPA (D _ _ _ P _ _ _ _ _ _ _ _ n A _ _ _ _ _ _ _ y)

6. DPO (D _ _ _ P _ _ _ _ _ _ _ _ n O _ _ _ _ _ r

7. EDPB (E _ _ _ _ _ _ n D _ _ _ P _ _ _ _ _ _ _ _ n B _ _ r _)

8. ICT (I _ _ _ _ _ _ _ _ _ _ n and C _ _ _ _ _ _ _ _ _ _ _ _ _ s T _ _ _ _ _ _ _ _ y)

9. ISP (I _ _ _ r_ _ _ S _ _ _ _ _ e P _ _ _ _ _ _ r)

10. PIN (P _ _ _ _ _ _ l I _ _ _ _ _ _ _ _ _ _ _ _ n N _ _ _ _ r)

11. SIS (S _ _ _ _ _ _ n I _ _ _ _ _ _ _ _ _ n S_ _ _ _ m)

12. PNR (P _ _ _ _ _ _ _ r N _ _ e R _ _ _ _ d)

13. SWIFT (S _ c _ _ _ y for W _ _ _ d w _ _ e I _ _ _ _ b _ _ k F _ _ _ _ _ _ _ l T _ _ _ c _ _ _ _ _ _ _ _ _ _ _ n)

14. SEPA (S_ _ _ _ e E _ _ o P _ _ _ _ n _ _ A _ _ a)

35 Sources: 1) European Union Agency for Fundamental Rights, 2014. Council of Europe, 2014; 2) Several EU documentation sources.

Unit 3

THE LANGUAGE OF DATA PROTECTION: CASES AND FUNDAMENTAL CONCEPTS.

INTRODUCTION

Flavius Iancu Motu

Which is the most relevant case law?

The CJEU has given numerous preliminary rulings on various topics in the field of personal data protection.

The notion of 'personal data' has gradually expanded in the rulings of the CJEU, encompassing now not only 'traditional' features, such as a natural person's name or his/her image, but also specific information, such as a natural person's tax data, or that natural person's computer IP address. Drawing an exhaustive list of such cases is next to impossible, yet the decisions in the cases C-101/01 (Lindquist), C-28/08 P (Bavarian Lager), C-291/12 (Schwartz) or C-201/14 (Bara) constitute landmark case law that remains relevant to the present day.

Defining the 'controller' and, respectively, the 'processor' have also been laborious tasks the CJEU has embarked on. From public authorities and governmental agencies to private entities and religious cults, the CJEU has expanded the scope of these notions through its successive judgments given in C-101/01 (Lindqvist), C-73/07 (Satakunnan Markkinapörssi and Satamedia), C-131/12 (Google Spain and Google), C-40/17 (Fashion ID) and C-25/17 (Jehovan todistajat).

The CJEU jurisprudence on the data subject's right has crystallized along the way, consolidating the position of the data subject against the actions of the controller. Following a constant protective approach, the CJEU has expanded the scope of the provisions laid down in the previous legal instrument, upholding the 'right to be forgotten' in its famous judgment given in the case C-131/12 (Google Spain and Google) and has invalidated the Directive 2006/24/EC in its judgment given in the Joined Cases C-293/12 (Digital Rights Ireland LTD) and C-594/12 (Kärntner Landesregierung). Moreover, the CJUE has declared the Commission's Decision no. 2000/520 (the Safe Harbour adequacy decision) invalid in its judgment handed down on the 6th of October 2015 in C-362/14 (Schrems / Digital Rights Ireland).

LANGUAGE EXERCISES

Exercise I. Online task: terminology and online recycling.

Read the text below.

Data Protection regulation at European level has become more and more necessary in the light of the recent technological development. However, the technology does not just bring more challenges in terms of regulation, it also brings opportunities and advantages for instance in the field of learning a language.

Test the potential of an open source online application used by masses of teachers and learners.

Quizlet is an effective way to study a wide range of questions for an unimaginable variety of subjects throughout all areas of education and life. It is powered by the Learning Assistant Platform which uses machine learning to process data from millions of anonymous study sessions, and then combines that data with proven techniques from cognitive science. By understanding how people really learn, this powerful platform drives studying that's more effective and more efficient, by only showing students material they need to learn — and making it fun at the same time.

Check this out: Data Protection Glossary[36]

https://quizlet.com/190771515/data-protection-vocabulary-flash-cards/

You can:

- listen to the terms and definitions online or offline on your PC, android, iPhone or any tablet;
- download the glossary in a form of flashcards or the handout with or without pictures;
- play games (matching, spelling, writing etc.) to practice and recycle the terminology to remember;
- test your language skills regarding the concerned terminology;
- and if you do not have online access, just do the following exercise: match the terminology with the best fitting definition or explanation.

36 On Quizlet by Denisa Petriláková.

	The Term	The Definition
1	Access Levels	refers to the quantities, characters, or symbols on which operations are performed by a computer.
2	The data processor	refers to different types of levels that give certain people access to different things.
3	Anti Virus Software	discloses personal data to one or more specific entities (other than the Data Subject, the Data Processor, or a Person Tasked with Processing) in whatever manner, such as by making the data available or accessible.
4	Access Levels	any information concerning natural persons that are or also can be identified by way of other items of information such as a number or an ID code.
5	Encrypt:	computers from viruses.
6	Data Protection Authority (DPA)	are determined by your importance.
7	Firewall is	allows you to retrieve lost or damaged data.
8	Anti Virus Software protects	is what you do to a file when you only want certain people to see it.
9	Communication	is the natural person, company, association or organization the Data Controller has entrusted with specific data processing management and control tasks on account of the relevant experience and/or skills.
10	Data is the term	is the software that is used to protect your PC.
11	Dissemination	is an administrative independent authority set up by the national laws. Similar authorities have been set up in all EU countries pursuant to Article 8 of the Charter of Fundamental Rights of the European Union.
12	Personal Data includes	refers to making personal data known to the public at large and/or to an indefinite amount of entities - for instance, by publishing personal data in a daily or posting personal data on a web page.
13	Backup Recovery	is something that is (hopefully) able to stop viruses.

Exercise II. Word building. The Costeja Gonzàlez case.

Fill in the gap with the most appropriate form (or tense) of the word in square brackets.

JUDGMENT OF THE COURT (Grand Chamber)

13 May 2014

"Personal data — **(1)** _____ [*protectorate*] of individuals with regard to the processing of such **(2)** _____ [*datum, plural form*]— Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — **(3)** _____ [*process*] of data contained on websites — Searching for, indexing and **(4)** _____ [*store*] of such data — Responsibility of the operator of the search engine — **(5)** _____ [*establish*] on the territory of a Member State — **(6)** _____ [*extend*] of that operator's obligations and of the data subject's rights — Charter of **(7)** _____ [*fundament*] Rights of the European Union — Articles 7 and 8"

In Case C131/12,

REQUEST for a preliminary **(8)** _____ [*rule*] under Article 267 TFEU from the Audiencia Nacional (Spain), made by **(9)** _____ [*decisive*] of 27 February 2012, received at the Court on 9 March 2012, in the **(10)** _____ [*proceed, plural form*]

Google Spain SL,

Google Inc.

v

Agencia Española de Protección de Datos (AEPD),

Mario Costeja González,

THE COURT (Grand Chamber),

(…)

gives the following

(11) _____ [*judge*]

(…)

The dispute in the main proceedings and the questions **(12)** _____ [*reference*] for a preliminary ruling

14 On 5 March 2010, Mr Costeja González, a Spanish national **(13)** _____ [*reside*] in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large **(14)** _____ [*circulate*], in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an **(15)** _____ [*announce*] mentioning Mr Costeja González's name appeared for a real-estate auction connected with **(16)** _____ [*attach*] proceedings for the recovery of social security debts.

15 By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or **(17)** _____ [*alteration*] those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. **(18)** _____ [*required*] to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been **(19)** _____ [*full*] resolved for a number of years and that reference to them was now **(20)** _____ [*entire*] irrelevant.

16 By **(21)** _____ [*decide*] of 30 July 2010, the AEPD rejected the **(22)** _____ [*complain*] in so far as it related to La Vanguardia, taking the view that the **(23)** _____ [*publish*] by it of the information in question was legally justified as it took place upon order of the **(24)** _____ [*Minister*] of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to **(25)** _____ [*security*] as many bidders as possible.

17 On the other hand, the complaint was **(26)** _____ [*uphold*] in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection **(27)** _____ [*legislative*] given that they carry out data **(28)** _____ [*process*] for which they are responsible and act as intermediaries in the information society.

The AEPD took the view that it has the power to require the **(29)** _____ [*withdraw*] of data and the prohibition of access to certain data by the operators of search engines when it considers that the **(30)** _____ [*location*] and dissemination of the data are **(31)** _____ [*liability*] to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to **(32)** _____ [*erasure*] the data or information from the website where they appear, including when **(33)** _____ [*retain*] of the information on that site is justified by a **(34)** _____ [*statute*] provision.

18 Google Spain and Google Inc. brought **(35)** _____ [*separation*] actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional **(36)** _____ [*joint*] the actions.

(…)

21 By Question 2(a) and (b), which it is appropriate to **(37)** _____ [*examination*] first, the **(38)** _____ [*refer*] court asks, in essence, whether Article 2(b) of Directive 95/46 **(39)** _____ [*be, interpret*] as meaning that the activity of a search engine as a **(40)** _____ [*provision*] of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of **(41)** _____ [*prefer*] must be classified as 'processing of personal data' within the meaning of that provision when that information contains personal data. If the answer is in the **(42)** _____ [*affirm*], the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

Language of the case: Spanish.

Exercise III. Rewrite the following sentences using the passive voice.

Source: Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

1. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantees this right.

2. Regulation (EU) 2016/679 provides for the adaptation of Regulation (EC) No 45/2001.

3. The Court of Justice of the European Union (the 'Court of Justice'), should interpret homogeneously those two sets of provisions.

4. The Commission should conduct a review of this Regulation.

5. This Regulation should cover the processing of administrative personal data, such as staff data, by Union bodies or agencies.

6. The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned.

7. A clear affirmative act should give consent.

8. The controller should establish time limits for erasure or for a periodic review.

9. The controller should verify the existence of a relevant ground for lawfully processing personal data.

10. Union law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

Exercise IV. Big Brother Watch v. Secretary of State [2018] ECHR 722.[37]

A recent case concerned with Data Protection decided by the ECHR:

TASK 1. Case study.

Task 1.1. Vocabulary.

Check out the meaning of the following expressions. Then read the case and use the expressions below to write down sentences to summarize the case.

- mass electronic surveillance
- to address key questions
- proportionality of bulk interception programmes
- the case was being deliberated
- to uphold a bulk surveillance programme
- a now-defunct Regulation
- to be deficient in important respects
- to be categorically disproportionate
- prior judicial authorization
- to be indispensable
- to enjoy a wide margin of appreciation
- the legitimate aim of protecting national security
- interception regimes - bulk or targeted
- be discerned from the relevant legislation
- objective evidence of reasonable suspicion
- the persons for whom data is being sought
- to render the operation impossible
- the related communications data
- an essential tool for the intelligence services

37 Based on: https://www.echr.coe.int/Documents/Press_Q_A_Brother_Watch_ENG.pdf

- the fight against terrorism
- the possibility of improper action
- a dishonest, negligent or over-zealous official
- to ensure compliance with Article 8 of the Convention.

Task 1.2. The facts of the case.

The European Court of Human Rights issued a highly anticipated blockbuster Chamber judgment in Big Brother Watch v. UK, nos. 58170/13, 62322/14, 24960/15.

It is the first **mass electronic surveillance** case to be decided against the UK after the Edward Snowden revelations, and it touches upon numerous issues. The judgment is nuanced, complex, and long.

It **addresses key questions** such as the p**roportionality of bulk interception programmes** much more directly and with greater sophistication than the recent judgment in Centrum för Rättvisa v. Sweden no. 35252/08, which was decided by a different Chamber while this **case was being deliberated**, and which also **upheld a bulk surveillance programme**.

The judgment is too rich to summarize easily, so we will only observe some key takeaways.

While the Court finds that the UK's surveillance programme under the **now-defunct Regulation of Investigatory Powers Act (RIPA)** was **deficient in important respects** and in violation of Article 8 and 10 of the Convention, it at the same time normalizes such mass surveillance programmes.

In particular, the Court decided that bulk interception programmes **are not categorically disproportionate**, as privacy activists have argued. Second, in a similar vein, the Court finds that **prior judicial authorization is not indispensable** for the legality of bulk interception even if prior judicial authorization could be seen as best practice.

The Court has expressly recognised that the national authorities **enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security**.

Nevertheless, as indicated previously, it is evident from the Court's case-law over several decades that all **interception regimes (both bulk and targeted)** have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot **be discerned from the relevant legislation**.

Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified minimum requirements that both bulk interception and other interception regimes must satisfy in order to be sufficiently foreseeable to minimise the risk of abuses of power.

The applicants argue that in the present case the Court should "update" those requirements by including requirements for **objective evidence of reasonable suspicion in relation to the persons for whom data is being sought**, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject.

In their view, such changes would reflect the fact that due to recent technological developments the interception of communications now has greater potential than ever before to paint an intimate and detailed portrait of a person's private life and behaviour.

However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that **the additional requirements proposed by the applicants might constitute important safeguards** in some cases, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand.

Bulk interception is by definition untargeted, and to require "reasonable suspicion" **would render the operation of such a scheme impossible**. Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime.

Judicial authorisation, by contrast, is **not inherently incompatible with the effective functioning of bulk interception.** Nevertheless, as the Venice Commission acknowledged in their report on the Democratic Oversight of Signals Intelligence Agencies, the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness".

The Court has found it "d**esirable to entrust supervisory jurisdiction to a judge"** because, as a result of the secret nature of the surveillance, the individual will usually be unable to seek a remedy of his or her own accord. However, that is not the case in every contracting State.

The Court has acknowledged that "**the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system**", and one need only look at its most recent jurisprudence to find examples of cases where prior judicial authorisation provided limited or no protection against abuse.

Therefore, while the Court considers judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it can neither be necessary nor sufficient t**o ensure compliance with Article 8 of the Convention.** Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse. Accordingly, the Court will examine the justification for any interference in the present case by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. It will also have regard to the additional relevant factors which it identified in Roman Zakharov, but did not classify as "minimum requirements"; namely, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

Consequently, while the Court does not doubt that **related communications data is an essential tool for the intelligence services in the fight against terrorism** and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content.

The Court also for the first time **directly examines the lawfulness of intelligence sharing, which it again normalizes while being wary of the possibility of abuse**:

Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts. Due to the nature of global terrorism, and in particular the

complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "**information flow"** was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society".

What do you think about the outcome of the case?

Write down a short text stating your opinions from your professional point of view focusing on the hypothetical outcome of such a case in your country. Use the concepts such as "regulated by the law", "principle of proportionality", "pursuing legitimate aim", etc.

Task 1.3. Summarizing and passive knowledge vocabulary building.

Read the extract summarizing the facts of the case either in writing or orally using your phone or a dictaphone to record your summary and then checking it against the text, underline the unknown or difficult expressions and if unsure use the following internet websites to check the meaning: go either to a Legal English Dictionary at ***https://www.translegal.com/legal-english-dictionary*** *or go to the following website of European Data Protection Supervisor and search for the terminology and write down the definitions.* ***https://edps.europa.eu/data-protection/data-protection/glossary_en).***

When you write or record the summary, it is really beneficial to prepare a list of those difficult expressions on the side and then try to include the expressions in the summary to attempt to upgrade your passive knowledge of the term into activating those terms via production.

Background of the Case

In 2013, Edward Snowden revealed that the UK intelligence agency GCHQ was running a mass surveillance and bulk communications interception programme known as TEMPORA. UK intelligence agencies were also receiving data from two other surveillance and bulk interception programmes, PRISM and UPSTREAM, run by the US National Security Agency (NSA).

Following these revelations, Big Brother Watch, English PEN, Open Rights Group and Dr Constanze Kurz made an application to the European Court of Human Rights on the grounds that these surveillance programmes were a significant interference with UK citizens' right to privacy under Article 8 of the European Convention on Human Rights. It is this case which is being heard by the Chamber.

The applications were introduced following revelations by Edward Snowden relating to the electronic surveillance programmes operated by the intelligence services of the United States of America and the United Kingdom.

The applicants all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from Communications Service Providers ("CSPs").

The case challenged the legality of the indiscriminate surveillance of UK citizens and the bulk collection of vast amounts of their personal information and communications by UK intelligence agencies (including GCHQ) under the legal regime set out in the Regulation of Investigatory Powers Act (RIPA) 2000.

The UK surveillance regime under RIPA was untargeted, meaning that UK citizens' private communications and information w**as collected at random without any element of suspicion or evidence of wrongdoing**, there was no authorization required for the interception of the communications, and process of interception was effective indefinitely.

We are challenging the RIPA regime on the grounds that there was no sufficient legal basis for such indiscriminate bulk interception, no defined limits on the exercise of the power and no adequate oversight – therefore, it infringed UK citizens' Article 8 right to a private life.

Specifically, the case questioned:

- whether the storage and searching of those intercepted communications is lawful;
- whether the use of computer programs to search this data is an interference with people's privacy;
- whether greater controls are needed on the receipt of intercepted foreign intelligence so that it doesn't circumvent UK safeguards; and
- whether it is fair that there are different standards applied to UK and non-UK residents.

Task 1.4.

Answer the questions either in writing or orally (again recording the answers) depending on which language skill you wish to practice. You may once again use a side list of terms and expressions you are aiming to activate. Then check the answers you have written or recorded against the text.

- Who was the data subject in the instant case?
- What was the stored data related to?
- What kind of data was collected?
- How was the data collected? In other words, was there any methodology, probable cause or a suspicion?
- What were the arguments of the data subjects?
- What were at least some of the legal questions the ECHR had to test?
- What was the decision of the ECHR?
- What was the reasoning underpinning the judgement?
- Do you personally find the arguments convincing?
- Can you explain the difference between targeted and bulk surveillance and data collection?
- Are you aware of data surveillance and collection schemes in your country?
- Would the police or the security agency in your country need a judicial authorization to collect data at random?
- What do you think about the outcome of the case?

TASK 2. Listening.[38] [39]

Watch the video in which the hearing in the instant case is being held in Strasbourg and answer the following questions:

- Who opens the hearing, is it declared if the hearing public and is it expressly stated if the hearing is on the admissibility or the merits of the case?
- Were all the applications lodged with the court simultaneously or not?
- Has a hearing in the instant case already been held?
- Has a judgement already been delivered in the instant case?
- What was the outcome of the motion to refer the case to the Grand Chamber of ECHR
- and what was such a request in compliance with?
- Who is first to deliver a statement? Who is this on behalf of?
- What opportunity is the Court presented in this case in the opinion of the legal counsel delivering the statement?
- What is Edward Snowden document said to have illuminated?
- Who are the concerned impugned general warrants authorized by?
- Do the warrants list the number of selectors of the collected data and what inference do the applicants make with respect to this fact?
- What is the general practice of the relevant agency of the Member state in terms of the length of the data storage?
- Is there a system of an independent prior approval with respect to the access to the concerned data?
- How many safeguards does the opposing party (the Government) rely on in order to justify the compatibility with the Convention (and which is the relevant Article)? Can you listen and name the safeguards (and the rebutting arguments of the applicants)?

TASK 3: Focus on vocabulary.

Read the text and choose the words that best fit the gap. Each word may be used only once:

extent	exempting	safeguards	balance
examines	communications	legitimate	wary
accessible	conveyance	shortcomings	flow

While the Court does not doubt that related **(1)** _____ data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair **(2)** _____ between the competing public and private interests by **(3)** _____ it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be **(4)** _____ for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require

38 (minutes 0:00 to 12:30 of the ECHR hearing)

39 Source: https://www.echr.coe.int/Pages/home.aspx?p=hearings&w=5817013_10072019&language=en&c=&py=2019

the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient **(5)** _____ in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the **(6)** _____ necessary to determine whether an individual is, for the time being, in the British Islands.

The Court also for the first time directly **(7)** _____ the lawfulness of intelligence sharing, which it again normalizes while being **(8)** _____ of the possibility of abuse.

Faced with such a threat, the Court has considered it **(9)** _____ for Contracting States to take a firm stand against those who contribute to terrorist acts. Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a **(10)** _____ of information between the security services of many countries in all parts of the world.

In light of the foregoing considerations, the Court considers that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicate with sufficient clarity the procedure for requesting either interception or the **(11)** _____ of intercept material from foreign intelligence agencies. In this regard, it observes that the high threshold recommended by the Venice Commission is met by the respondent State's regime. The Court further observes that there is no evidence of any significant **(12)** _____ in the application and operation of the regime.

TASK 4. Searching for sources.[40] [41]

Go to the ECHR website and check out what information and data is available on this specific case.

Question: *What do you believe might be expected in terms of developments in the instant case?*

Reflection: Think about whether, in a hypothetically identical case, the applicant in your country could collect the data without the authorization of the court or whether your national law would prevent such a course of action.

40 Source: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-186048%22]}

41 https://www.supremecourt.uk/cases/uksc-2013-0114.html

ANSWER KEYS

UNIT 1. LANGUAGE

Exercise I.

1. personal data; 2. identifiable person; 3. processing of personal data; 4. personal data filing system; 5. controller; 6. third party; 7. data subject consent; 8. data protection authority; 9. dissemination; 10. encryption; 11. firewall; 12. hacker; 13. judicial data; 14. recipient; 15. personal safety measures; 16. privacy; 17. remedy; 18. security measures; 19. recovery; 20. data processor.

[6]

Exercise II.

1. c (to); 2. a (from); 3. b (to); 4. a (to); 5. a (of); 6. c (to); 7. a (in); 8. a (for); 9. a (from); 10. a (to); 11. c (with); 12. b (about); 13. b (for); 14. a (to); 15. a (to); 16. a (by); 17. c (on); 18. b (by); 19. a (in); 20. b (Ø).

Exercise III.

Task 1. Open answers.

Task 2. 1. A submission submitted with a court - a filing; 2. The devices or the instruments of achieving something - the means; 3. Deliberately - intentionally; 4. The way of getting to something - an access; 5. A person connected to one by family ties - a relative; 6. Something related to a person - personal; 7. To be covered by a definition or a concept - to fall within; 8. The judge or a panel of judges decided - the court held; 9. Employees, staff - personnel; 10. An idea to do something deliberately to - an intent.

Task 3. Open answers.

Task 4.

Data subject means an individual who is the subject (1) of personal data. Data controller means a person who (either alone or jointly or (2) in common with other persons) determines the purposes (3) for which and the manner in which any personal data are, or are to be, processed.

In relation to data controllers, the term (4) jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently (5) of each other.

Data processor, in relation to personal data, means any person (other (6) than an employee of the data controller) (7) who processes the data on behalf of the data controller.

Data processors are not directly subject (8) to the Act. However, most data processors, if not all, will be data controllers in (9) their own right for the processing they do for their own administrative purposes, such (10) as employee administration or sales.

Task 5.

Case studies to practice writing. Answer to case 1: Yes, information held on the microfiche records is personal data. 2. Answer to case 2: Yes, the government department and the councils are data controllers in common in relation to the personal data on the database.

Case studies to practice speaking. Answer to case 1: Yes, the council and the police are joint data controllers in relation to personal data processed in operating the system. Answer to case 2: The utilities company remains the data controller. The company that operates the call centre is a data processor.

ADDITIONAL LANGUAGE PRACTICE

Exercise I.

(1) aggregated; (2) personal; (3) commercial; (4) necessary; (5) punishable; (6) timely; (7) consistency; (8) analytical; (9) private; (10) core; (11) primary; (12) ancillary; (13) identified; (14) identifiable; (15) useful; (16) anonymous.

Exercise II.

A. Are the following statements True or False?

1. F; 2. T; 3. F; 4. T; 5. T; 6. F; 7.T; 8. F.

B. What word/phrase is being described?

1. indictment; 2. cracker; 3. intrusion; 4. dark net; 5. acquaintances; 6. hackers; 7. obstruction of justice.

C. Find a synonym for the words underlined

1. given court judgment; 2. parole; 3. part of deep net, part of web not indexed by search engines.

4. operation; 5. to custom-make.

Exercise III.

Reading 1.

1. enshrined; 2. streamlining; 3. strengthen; 4. consent; 5. retaining; 6. breaches; 7. default.

Reading 2.

Part 1.

1. designated; 2. ensures; 3. set forth; 4. issued; 5. endorsed.

Part 2.

1. timely; 2. processing; 3. expertise; 4. highest; 5. secrecy; 6. official; 7. suffer; 8. competent; 9. eligible; 10. body.

Part 3.

1. provisions; 2. compliance; 3. policies; 4. processor; 5. awareness; 6. audits; 7. communication; 8. doubt; 9. consultation; 10. competence; 11. staff; 12. concern.

Part 4. Open answers.

Part 5.

1. synergy; 2. limited powers; 3. complaints and queries; 4. investigation and resolution; 5. fear; 6. own - initiative; 7. framework; 8. valuable partner.

Part 6. Open answers.

UNIT 2. LANGUAGE

Exercise I.

Task 1.

1. (a) fairness/transparency; (b) incompatible; (c) minimisation; (d) inaccurate/delay; (e) longer/subject; (f) unauthorized/confidentiality; 2. compliance.

Task 2.

(1) to; (2) to; (3) at; (4) into; (5) with; (6) out; (7) in; (8) to.

Task 3.

(a) lawfully/fairly; (b) explicit/incompatible; (c) adequate; (d) inaccurate; (f) appropriate/accidental.

Task 4.

(a) transparent; (b) covert; (c) surveillance; (d) threats; (e) due; (f) notion; (g) explicit; (h) erasure.

Task 5.

(1) human intervention; (2) electronic mail; (3) direct marketing; (4) national legislation; (5) unsolicited communications.

Task 6.

[1] safeguard; [2] conjunction; [3] breach; [4] override; [5] malicious; [6] denial.

Task 7.

1. **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

2. **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

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

where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

4. **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

5. **'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

6. '**personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

7. **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

8. **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

10. **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

11. **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Exercise II.

(1) data; (2) reasonable; (3) verify; (4) lawfulness; (5) concerning; (6) examination; (7) provided; (8) are processed; (9) logic; (10) profiling; (11) adversely; (12) intellectual; (13) refusal; (14) quantity; (15) is delivered; (16) concerning; (17) retention; (18) necessary; (19) relevant; (20) lawful; (21) freedom; (22) compliance; (23) performance; (24) authority; (25) historical; (26) statistical; (27) defence.

ADDITIONAL LANGUAGE EXERCISES

Exercise I.

1a. acquired; 1b. acquiesced

2a. resume; 2b. adjourn

3a. advice; 3b. advise

4a. sanction (prohibit); 4b. sanction (allow)

5a. proceedings; 5b. procedure

6a. remind; 6b. remember

7a. specially; 7b. especially

8a. save (*help*); 8b. save (*except for*)

Exercise II.

1. personal data; 2. injured party; 3. right to be forgotten; 4. infringement procedure; 5. applicable law; 6. appropriate measures; 7. systematic monitoring; 8. enforceable judgment; 9. appropriate safeguards; 10. authentic instruments; 11. data portability; 12. DPO independence.

Exercise III.

Task 1. 1. expression; 2. repeal; 3. adapting; 4. application; 5. burdens.

Task 2. 1. attention; 2. restrict; 3. national; 4. obligation; 5. application; 6. enforcement; 7. courts; 8. interpretation.

Exercise IV.

1. Closed Circuit Television; 2. Customs Information System; 3. European Data Protection Supervisor; 4. Central Schengen Information System; 5. Data Protection Authority.; 6. Data Protection Officer; 7. European Data Protection Board; 8. Information and Communications Technology; 9. Internet Service Provider; 10. Personal Identification Number; 11. Schengen Information System; 12. Passenger Name Record; 13. Society for Worldwide Interbank Financial Telecommunication; 14. Single Euro Payments Area.

UNIT 3

LANGUAGE

Exercise I.

The term **The definition**

1. Access Levels – refer to different types of levels that give certain people access to different things.
2. The data processor – is the natural person, company, association or organization the Data Controller has entrusted with specific data processing management and control tasks on account of the relevant experience and/or skills.
3. Anti-Virus Software – is the software that is used to protect your PC.
4. Access Levels – "are determined by your importance".
5. Encrypt "is what you do to a file when you only want certain people to see it".
6. Data Protection Authority (DPA) – "is an administrative independent authority set up by the national laws. Similar authorities have been set up in all EU countries pursuant to Article 8 of the Charter of Fundamental Rights of the European Union".
7. Firewall – is something that is (hopefully) able to stop viruses.
8. Anti-Virus Software protects – "computers from viruses".
9. Communication – discloses personal data to one or more specific entities (other than the Data Subject, the Data Processor, or a Person Tasked with Processing) in whatever manner, also by making the data available or accessible.
10. Data is the term – "that refers to the quantities, characters, or symbols on which operations are performed by a computer."
11. Dissemination – refers to -making personal data known to the public at large and/or to an indefinite amount of entities - for instance, by publishing personal data in a daily or posting personal data on a web page.
12. Personal Data includes – "any information concerning natural persons that are or also can be identified also by way of other items of information such as a number or an ID code".
13. Backup Recovery – allows you to retrieve lost or damaged data.

Exercise II.

1. protection; 2. data; 3. processing; 4. storage; 5. establishment; 6 extent; 7. fundamental; 8. ruling; 9. decision; 10. proceedings; 11. judgment; 12. referred; 13. resident; 14. circulation; 15. announcement; 16. attachment; 17. alter; 18. be required; 19. fully; 20. entirely; 21. decision; 22. complaint; 23. publication; 24. ministry; 25. secure; 26. upheld; 27. legislation; 28. information; 29. withdrawal; 30. locating; 31. liable; 32. erase; 33. retention; 34. statutory; 35. separate; 36. joined; 37. examine; 38. referring; 39. be interpreted; 40. provider; 41. preference; 42. affirmative.

Exercise III.

1. This right is guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.
2. The adaptation of Regulation (EC) No 45/2001 is provided for by Regulation (EU) 2016/679.
3. Those two sets of provisions should be interpreted homogeneously by the Court of Justice of the European Union (the 'Court of Justice').
4. A review of this Regulation should be conducted by the Commission.
5. The processing of administrative personal data, such as staff data, by Union bodies or agencies, should be covered by this Regulation.
6. The risks to the data subjects concerned can be reduced by the application of pseudonymisation to personal data.
7. Consent should be given by a clear affirmative act.
8. Time limits should be established by the controller for erasure or for a periodic review.
9. The existence of a relevant ground for lawfully processing personal data should be verified by the controller.
10. The tasks and purposes for which the further processing should be regarded as compatible and lawful may be determined by Union law.

Exercise IV.

Tasks 1.1; 1.2; 1.3; 1.4. Open answers

Task 2. Open answers.

Task 3. Focus on vocabulary.

(1) communications; (2) balance; (3) exempting; (4) accessible; (5) safeguards; (6) extent; (7) examines; (8) wary; (9) legitimate; (10) flow; (11) conveyance; (12) shortcomings.

Task 4. Open answers.

GLOSSARY OF TERMS

The glossary contains the official terms found in the GDPR.[42]

(1) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(2) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(3) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(4) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(5) 'cross-border processing' means either:

a. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

b. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(6) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(7) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(8) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

42 Source: GDPR - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) published in the Official Journal of the European Union, L 119, 4 May 2016.

(9) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(10) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(11) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);

(12) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

(13) 'main establishment' means:

a. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

b. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(14) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(15) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(16) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(17) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(18) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work,

economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(19) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(20) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(21) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(22) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(23) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(24) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(25) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

a. the controller or processor is established on the territory of the Member State of that supervisory authority;

b. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

c. a complaint has been lodged with that supervisory authority;

(26) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

SUMMARY OF CASES

1. DATA PROTECTION: DEFINITIONS AND CONCEPTS

1.1. PERSONAL DATA: (Art. 4.1. GDPR[43]):

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

CJEU jurisprudence:

a) C-101/01 (Lindquist) (ECLI:EU:C:2003:596): "The name of a person in conjunction with his/her telephone number, and information about his/her working conditions or hobbies constitute personal data."

b) C-73/07 (Satakunnan Markkinapörssi and Satamedia) (ECLI:EU:C:2008:727): "The surname and given name of certain natural persons whose income exceeds certain thresholds, as well as the amount of their earned and unearned income, constitute personal data" [includes personal data that have already been published in unaltered form in the media].

c) C-28/08 P (Bavarian Lager) (ECLI:EU:C:2010:378): "Surnames and forenames may be regarded as personal data. Thus the list of names of participants in a meeting is personal data, since persons can be identified."

d) T-496/13 (McCullough) (ECLI:EU:T:2015:374) "Surnames are personal data and therefore are protected by Regulation 45/2001. The fact that the members of Cedefop's decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, and that the surnames were published in the OJ or on the internet, does not affect the characterization of the surnames as personal data."

e) C-141/12, C-372/12 (M) (ECLI:EU:C:2014:2081): "The data relating to the applicant for a residence permit included in the minute (applicant's name, date of birth, nationality, gender, ethnicity, religion and language) constitute personal data. The legal analysis in

43 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) published in the Official Journal of the European Union, L 119, 4 May 2016.

the minute may contain personal data but it does not in itself constitute such data. The legal analysis is not information relating to the applicant, but at most, in so far as not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation. This interpretation is consistent with the language of Article 2(a) and the objective and general scheme of Directive 95/46."

f) C-291/12 (Schwartz) (ECLI:EU:C:2013:670): "Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows them to be identified with precision."

g) C-342/12 (Worten) (ECLI:EU:C:2013:355): Data contained in the record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent "information relating to an identified or identifiable natural person."

h) C-473/12 (Englebert) (ECLI:EU:C:2013:715): "Data collected by private detectives relating to persons acting as estate agents concern identified or identifiable natural persons, and therefore constitute personal data."

i) C-212/13 (Rynes) (ECLI:EU:C:2014:2428): "The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned. "

j) C-201/14 (Bara) (ECLI:EU:C:2015:638): "Tax data transferred are personal data, since they are "information relating to an identified or identifiable natural person."

k) C-615/13 P (Client Earth) (ECLI:EU:C:2015:489): "The information as to which expert is the author of each comment made by the external experts constitutes information which falls within the scope of personal data. The fact that the information is provided as part of a professional activity does not mean that it cannot be characterized as personal data. The concepts of personal data and data relating to private life are not to be confused. The claim that the information concerned does not fall within the scope of private life is therefore ineffective. Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance were made public on the EFSA website does not mean such data cannot be characterized as personal data. Finally, characterization of information relating to a person as personal data does not depend on whether the person objects to the disclosure of that information."

l) T-259/03 (Nikolaou) (ECLI:EU:T:2007:254): "The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity."

m) C-70/10 (Scarlet Extended) (ECLI:EU:C:2011:771): "ISP addresses" [static IP addresses] "are protected personal data because they allow the related users to be precisely identified".

n) C-582/14 (Breyer) (ECLI:EU:C:2016:779): "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."

o) C-434/16 (Nowak) (ECLI:EU:C:2017:994): "the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data".

1.2. PROCESSING: (Art. 4.2. GDPR[44]):

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

CJEU jurisprudence:

a) C-131/12 (Google Spain and Google) (ECLI:EU:C:2014:317): "the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and … the operator of the search engine must be regarded as the 'controller' in respect of that processing.."

b) C-40/17 (Fashion ID) (ECLI:EU:C:2019:629): the embedding on a website of a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor constitutes processing;

c) C-345/17 (Buivids) (ECLI:EU:C:2019:122): "the video recording of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, may constitute a processing of personal data solely for journalistic purposes, within the meaning of that provision, in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public…"

d) C-212/13 (Rynes) (ECLI:EU:C:2014:2428): "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"; [According to Art. 2.2.c GDPR[45] does not apply to the processing of personal data: by a natural person in the course of a purely personal or household activity;]

e) Joined cases C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk and Others) (ECLI:EU:C:2003:294): "the data at issue in the main proceedings, which relate both to the monies paid by certain bodies and the recipients, constitute personal data …, being information relating to an identified or identifiable natural person'. Their recording and use by the body concerned, and their transmission to the Rechnungshof and inclusion by the latter in a report intended to be communicated to various political institutions and widely diffused, constitute processing of personal data."

f) C-101/01 (Lindqvist) (ECLI:EU:C:2003:596): "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means…"

44 See footnote 43, above.
45 See footnote 43, above.

g) C-73/07 (Satakunnan Markkinapörssi and Satamedia) (ECLI:EU:C:2008:727): an activity in which data on the earned and unearned income and the assets of natural persons are:

- collected from documents in the public domain held by the tax authorities and processed for publication;
- published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists,
- transferred onward on CD-ROM to be used for commercial purposes, and
- processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person,

must be considered as the 'processing of personal data' within the meaning of that provision… these activities … relating to data from documents which are in the public domain under national legislation, must be considered as activities involving the processing of personal data carried out 'solely for journalistic purposes', within the meaning of that provision, if the sole object of those activities is the disclosure to the public of information, opinions or ideas.

1.3. CONTROLLER: (Art. 2.7 GDPR[46]):

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

CJEU jurisprudence:

a) C-131/12 (Google Spain and Google) (ECLI:EU:C:2014:317): "the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and … the operator of the search engine must be regarded as the 'controller' in respect of that processing.."

b) T-670/16 (Digital Rights Ireland v Commission) (ECLI:EU:T:2017:838): "where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services. However, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service."

c) C-210/16 (Wirtschaftsakademie Schleswig-Holstein) (ECLI:EU:C:2018:388): "the admin-

46 See footnote 43, above.

istrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland…"; "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."

d) C-25/17 (Jehovan todistajat) (ECLI:EU:C:2018:551): "a religious community is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing."

e) C-40/17 (Fashion ID) (ECLI:EU:C:2019:629): "The operator of a website,…, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor can be considered to be a controller … . That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue."

1.4. PROCESSOR (Art. 4.8. GDPR[47]):

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

CJEU jurisprudence:

a) C-119/12 (Probst) (ECLI:EU:C:2012:748): "[the] processor acts only on the controller's instructions and […] the controller ensures compliance with the measures agreed in order to protect personal data against any form of unlawful processing"

Article 29 Data Protection Working Party

b) Opinion 1/2010 on the concepts of "controller" and "processor"[48]: "Two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf"

47 See footnote 43, above.

48 ARTICLE 29 DATA PROTECTION WORKING PARTY, "*Opinion 1/2010 on the concepts of „controller" and „processor" Adopted on 16 February 2010*" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf accessed 3 October 2019.

2. E-PRIVACY & PROTECTION OF PERSONAL DATA IN THE LAW ENFORCEMENT SECTOR

2.1. Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others) (ECLI:EU:C:2014:238)

(Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof)

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

Judgment of the Court (Grand Chamber), 8 April 2014

THE QUESTIONS:

Case C-293/12

On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 … and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?

and/or

(b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?'

Case C–594/12

The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.

In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation … No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?'

By decision of the President of the Court of 11 June 2013, Cases C-293/12 and C-594/12 were joined for the purposes of the oral procedure and the judgment.

CJEU held:

"As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time

period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection

and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).

Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."

On those grounds, the Court ruled:

"Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid."

2.2. Joined Cases C-203/15 and C-698/15 (Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others) (ECLI:EU:C:2016:970)

(Requests for a preliminary ruling from the Kammarrätten i Stockholm and the Court of Appeal (England & Wales) (Civil Division))

(Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law)

Judgment of the Court (Grand Chamber), 21 December 2014

THE QUESTIONS:

Case C-203/15

On 9 April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the PTS (the Swedish Post and Telecom Authority) that, following the ruling in the judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12; 'the Digital Rights judgment', EU:C:2014:238) that Directive 2006/24 was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the LEK (the Swedish Law (2003:389) on electronic communications), and that it would erase data retained prior to that date.

On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority, Sweden) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned.

On 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of the Digital Rights judgment. In a report dated 13 June 2014, entitled 'Datalagring, EU-rätten och svensk rätt, Ds 2014:23' (Data retention, EU law and Swedish law; 'the 2014 report'), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('the ECHR'). The special reporter emphasised that the Digital Rights judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should the Digital Rights judgment be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances in order to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.

On that basis, on 19 June 2014 the PTS informed Tele2 Sverige that it was in breach of its obligations under the national legislation in failing to retain the data covered by the LEK for six months, for the purpose of combating crime. By an order of 27 June 2014, the PTS ordered Tele2 Sverige to commence, by no later than 25 July 2014, the retention of that data.

Tele2 Sverige considered that the 2014 report was based on a misinterpretation of the Digital Rights judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the Förvaltningsrätten i Stockholm (Administrative Court, Stockholm) challenging the order of 27 June 2014. Since that court dismissed the action, by judgment of 13 October 2014, Tele2 Sverige brought an appeal against that judgment before the referring court.

In the opinion of the referring court, the compatibility of the Swedish legislation with EU law should be assessed with regard to Article 15(1) of Directive 2002/58. While that directive establishes the general rule that traffic and location data should be erased or made anonymous when no longer required for the transmission of a communication, Article 15(1) of that directive introduces a derogation from that general rule since it permits the Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, EU law allows, in certain situations, the retention of electronic communications data.

The referring court nonetheless seeks to ascertain whether a general and indiscriminate obligation to retain electronic communications data, such as that at issue in the main proceedings, is compatible, taking into consideration the Digital Rights judgment, with Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 and Article 52(1) of the Charter. Given that the opinions of the parties differ on that point, it is necessary that the Court give an unequivocal ruling on whether, as maintained by Tele2 Sverige, the general and indiscriminate retention of electronic communications data is per se incompatible with Articles 7 and 8 and Article 52(1) of the Charter, or whether, as stated in the 2014 Report, the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention.

In those circumstances the Kammarrätten i Stockholm (Administrative Court of Appeal of Stockholm, Sweden) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

'(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

(a) access by the national authorities to the retained data is determined as [described in paragraphs 19 to 36 of the order for reference], and

(b) data protection and security requirements are regulated as [described in paragraphs 38 to 43 of the order for reference], and

(c) all relevant data is to be retained for six months, calculated as from the day when the communication is ended, and subsequently erased as [described in paragraph 37 of the order for reference]?'

Case C-698/15

Mr Watson, Mr Brice and Mr Lewis each lodged, before the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) (United Kingdom), applications for judicial review of the legality of Section 1 of DRIPA (the UK Data Retention and Investigatory Powers Act 2014), claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter and Article 8 of the ECHR.

By judgment of 17 July 2015, the High Court of Justice (England & Wales), Queen's Bench Division (Divisional Court) held that the Digital Rights judgment laid down 'mandatory requirements of EU law' applicable to the legislation of Member States on the retention of communications data and access to such data. According to the High Court of Justice, since the Court, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. It follows from the underlying logic of the Digital Rights judgment that legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, Section 1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.

The Secretary of State for the Home Department brought an appeal against that judgment before the Court of Appeal (England & Wales) (Civil Division) (United Kingdom).

That court states that Section 1(1) of DRIPA empowers the Secretary of State for the Home Department to adopt, without any prior authorisation from a court or an independent administrative body, a general regime requiring public telecommunications operators to retain all data relating to any postal service or any telecommunications service for a maximum period of 12 months if he/she considers that such a requirement is necessary and proportionate to achieve the purposes stated in the United Kingdom legislation. Even though that data does not include the content of a communication, it could be highly intrusive into the privacy of users of communications services.

In the order for reference and in its judgment of 20 November 2015, delivered in the appeal procedure, wherein it decided to send to the Court this request for a preliminary ruling, the referring court considers that the national rules on the retention of data necessarily fall within the scope of Article 15(1) of Directive 2002/58 and must therefore conform to the requirements of the Charter. However, as stated in Article 1(3) of that directive, the EU legislature did not harmonise the rules relating to access to retained data.

As regards the effect of the Digital Rights judgment on the issues raised in the main proceedings, the referring court states that, in the case that gave rise to that judgment, the Court was considering the validity of Directive 2006/24 and not the validity of any national legislation. Having regard, inter alia, to the close relationship between the retention of data and access to that data, it was essential that that directive should incorporate a set of safeguards and that the Digital Rights judgment should analyse, when examining the lawfulness of the data retention regime established by that directive, the rules relating to access to that data. The Court had not therefore intended to lay down, in that judgment, mandatory requirements applicable to national legislation on access to data that does not implement EU law. Further, the reasoning

of the Court was closely linked to the objective pursued by Directive 2006/24. National legislation should, however, be assessed in the light of the objectives pursued by that legislation and its context.

As regards the need to refer questions to the Court for a preliminary ruling, the referring court draws attention to the fact that, when the order for reference was issued, six courts in other Member States, five of those courts being courts of last resort, had declared national legislation to be invalid on the basis of the Digital Rights judgment. The answer to the questions referred is therefore not obvious, although the answer is required to give a ruling on the cases brought before that court.

In those circumstances, the Court of Appeal (England & Wales) (Civil Division) decided to stay the proceedings and to refer to the Court the following questions for a preliminary ruling:

'(1) Does [the Digital Rights judgment] (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter]?

(2) Does [the Digital Rights judgment] expand the scope of Articles 7 and/or 8 of [the Charter] beyond that of Article 8 of the European Convention of Human Rights … as established in the jurisprudence of the European Court of Human Rights …?'"

CJEU held:

The first question in Case C-203/15

"… it is clear from the explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 final), which led to Directive 2002/58, that the EU legislature sought 'to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used'.

[…]

Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services (see, to that effect, judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraphs 47 and 48). As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

[…]

It must, in that regard, be observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers (see, to that effect, judgment of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraph 53). That list of objectives is exhaustive, as is apparent from the second sentence

of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision.

[…]

As regards whether national legislation, such as that at issue in Case C-203/15, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24.

The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the Digital Rights judgment, paragraph 26).

That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 37).

Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 28).

Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 60).

Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51).

In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).

Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 59).

National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).

Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical

areas, a high risk of preparation for or commission of such offences.

The second question in Case C-203/15 and the first question in Case C-698/15

In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 61).

Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (see, by analogy, ECtHR, 4 December 2015, Zakharov v. Russia, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80).

Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 95).

With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 66 to 68).

In any event, the Member States must ensure review, by an independent authority, of compliance with

the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the Digital Rights judgment, paragraph 68, and the judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 41 and 58).

On those grounds, the Court ruled:

"1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."

2.3. C-207/16 (Ministerio Fiscal) (ECLI:EU:C:2018:788)

(Requests for a preliminary ruling from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain)

(Electronic communications — Processing of personal data — Directive 2002/58/EC — Articles 1 and 3 — Scope — Confidentiality of electronic communications — Protection — Article 5 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Data processed in connection with the provision of electronic communications services — Access of national authorities to the data for the purposes of an investigation — Threshold of seriousness of an offence capable of justifying access to the data)

Judgment of the Court (Grand Chamber), 2 October 2018

THE QUESTIONS:

Mr Hernandez Sierra lodged a complaint with the police for a robbery, which took place on 16 February 2015, during which he was injured and his wallet and mobile telephone were stolen. On 27 February 2015, the police requested the investigating magistrate to order various providers of electronic communications services to provide (i) the telephone numbers that had been activated between 16 February and 27 February 2015 with the International Mobile Equipment Identity code ('the IMEI code') of the stolen

mobile telephone and (ii) the personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as their surnames, forenames and, if need be, addresses.

By order of 5 May 2015, the investigating magistrate refused that request. The latter held that the measure requested would not serve to identify the perpetrators of the offence. Moreover, it refused to grant the request on the ground that Law 25/2007 limited the communication of the data retained by the providers of electronic communications services to serious offences. Under the Criminal Code, serious offences are punishable by a term of imprisonment of more than five years, whereas the facts at issue in the main proceedings did not appear to constitute such an offence.

The Public Prosecutor's Office appealed against that order before the referring court, claiming that communication of the data at issue ought to have been allowed by reason of the nature of the facts and pursuant to a judgment of the Tribunal Supremo (Supreme Court, Spain) of 26 July 2010 relating to a similar case.

The referring court explains that, subsequent to that order, the Spanish legislature amended the Code of Criminal Procedure by adopting Organic Law 13/2015. That legislation, which is relevant to the resolution of the case in the main proceedings, introduced two new alternative criteria for determining the degree of seriousness of an offence. The first is a substantive criterion, relating to conduct which corresponds to criminal classifications the criminal nature of which is specific and serious, and which is particularly harmful to individual and collective legal interests. Moreover, the national legislature relied on a formal normative criterion, based on the penalty prescribed for the offence in question. The threshold of three years' imprisonment envisaged by that criterion does, however, cover the great majority of offences. In addition, the referring court considers that the State's interest in punishing criminal conduct cannot justify disproportionate interferences with the fundamental rights enshrined in the Charter.

In that regard, the referring court considers that, in the main proceedings, Directives 95/46 and 2002/58 establish a link with the Charter. The national legislation at issue in the main proceedings therefore comes within its scope, in accordance with Article 51(1) of the Charter, despite the fact that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 (OJ 2006 L 105, p. 54) was annulled by the judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238).

In that judgment, the Court recognised that the retention and communication of traffic data constitute particularly serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter and established criteria for the assessment of whether the principle of proportionality has been observed, including the seriousness of the offences warranting the retention of data and access thereto for the purposes of an investigation.

In those circumstances, the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Can the sufficient seriousness of offences, as a criterion which justifies interference with the fundamental rights recognised by Articles 7 and 8 of the [Charter], be determined taking into account only the sentence which may be imposed in respect of the offence investigated, or is it also necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally protected interests?

(2) If it were in accordance with the constitutional principles of the European Union, used by the Court of Justice in its judgment [of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238] as standards for the strict review of [Directive 2002/58], to determine the seriousness of the offence solely on the basis of the sentence which may be imposed, what should the minimum threshold be? Would it be compatible with a general provision setting a minimum of three years' imprisonment?'

CJEU held:

"… the referring court is uncertain as to the factors that should be taken into consideration in order to assess whether the offences in respect of which the police may be authorised, for the purposes of an investigation, to have access to personal data retained by providers of electronic communications services are sufficiently serious to warrant the interference entailed by such access with the fundamental rights enshrined in Articles 7 and 8 of the Charter, as interpreted by the Court in its judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238), and in Tele2 Sverige and Watson and Others.

As to the existence of an interference with those fundamental rights, it should be borne in mind, as observed by the Advocate General in points 76 and 77 of his Opinion, that the access of public authorities to such data constitutes an interference with the fundamental right to respect for private life, enshrined in Article 7 of the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. Such access also constitutes interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter, as it constitutes processing of personal data (see, to that effect, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, points 124 and 126 and the case-law cited).

As regards the objectives that are capable of justifying national legislation, such as that at issue in the main proceedings, governing the access of public authorities to data retained by providers of electronic communications services and thereby derogating from the principle of confidentiality of electronic communications, it must be borne in mind that the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, as a result of which that access must correspond, genuinely and strictly, to one of those objectives (see, to that effect, Tele2 Sverige and Watson and Others, paragraphs 90 and 115).

As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, it should be noted that the wording of the first sentence of Article 15(1) of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally.

In that regard, the Court has admittedly held that, in areas of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned (see, to that effect, Tele2 Sverige and Watson and Others, paragraph 99).

However, the Court explained its interpretation by reference to the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails (see, to that effect, Tele2 Sverige and Watson and Others, paragraph 115).

In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'.

By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.

It should therefore, first of all, be determined whether, in the present case, in the light of the facts of the case, the interference with fundamental rights enshrined in Articles 7 and 8 of the Charter that police access to the data in question in the main proceedings would entail must be regarded as 'serious'.

In that regard, the sole purpose of the request at issue in the main proceedings, by which the police seeks, for the purposes of a criminal investigation, a court authorisation to access personal data retained by providers of electronic communications services, is to identify the owners of SIM cards activated over a period of 12 days with the IMEI code of the stolen mobile telephone. As noted in paragraph 40 of

the present judgment, that request seeks access to only the telephone numbers corresponding to those SIM cards and to the data relating to the identity of the owners of those cards, such as their surnames, forenames and, if need be, addresses. By contrast, those data do not concern, as confirmed by both the Spanish Government and the Public Prosecutor's Office during the hearing, the communications carried out with the stolen mobile telephone or its location.

It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.

In those circumstances, access to only the data referred to in the request at issue in the main proceedings cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned.

[…] the interference that access to such data entails is therefore capable of being justified by the objective, to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious'."

On those grounds, the Court ruled:

"Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter of Fundamental Rights, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime."

2.4. C-40/17 (Fashion ID) (ECLI:EU:C:2019:629)

(Requests for a preliminary ruling the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany))

(Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Article 2(d) — Notion of 'controller' — Operator of a website who has embedded on that website a social plugin that allows the personal data of a visitor to that website to be transferred to the provider of that plugin — Article 7(f) — Lawfulness of data processing — Taking into account of the interest of the operator of the website or of that of the provider of the social plugin — Articles 2(h) and 7(a) — Consent of the data subject — Article 10 — Informing the data subject — National legislation allowing consumer-protection associations to bring or defend legal proceedings)

THE QUESTIONS:

"Fashion ID, an online clothing retailer, embedded on its website the 'Like' social plugin from the social network Facebook ('the Facebook "Like" button').

It is apparent from the order for reference that one feature of the internet is that, when a website is visited, the browser allows content from different sources to be displayed. Thus, for example, photos, videos, news and the Facebook 'Like' button at issue in the present case can be linked to a website and appear there. If a website operator intends to embed such third-party content, he places a link to the external content on that website. When the browser of a visitor to that website encounters such a link, it requests the content from the third-party provider and adds it to the appearance of the website at the desired place. For this to occur, the browser transmits to the server of the third-party provider the IP address of that visitor's computer, as well as the browser's technical data, so that the server can establish the format in which the content is to be delivered to that address. In addition, the browser transmits information relating to the desired content. The operator of a website embedding third-party content onto that website cannot control what data the browser transmits or what the third-party provider does with those data, in particular whether it decides to save and use them.

With regard, in particular, to the Facebook 'Like' button, it seems to be apparent from the order for reference that, when a visitor consults the website of Fashion ID, that visitor's personal data are transmitted to Facebook Ireland as a result of that website including that button. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not he or she is a member of the social network Facebook or has clicked on the Facebook 'Like' button.

Verbraucherzentrale NRW, a public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data.

Verbraucherzentrale NRW brought legal proceedings for an injunction before the Landgericht Düsseldorf (Regional Court, Düsseldorf, Germany) against Fashion ID to force it to stop that practice.

By decision of 9 March 2016, the Landgericht Düsseldorf (Regional Court, Düsseldorf) upheld in part the requests made by Verbraucherzentrale NRW, after having found that it has standing to bring proceedings under Paragraph 8(3)(3) of the UWG [the Gesetz gegen den unlauteren Wettbewerb (Law against unfair competition)].

Fashion ID brought an appeal against that decision before the referring court, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). Facebook Ireland intervened in that appeal in support of Fashion ID. Verbraucherzentrale NRW brought a cross-appeal seeking an extension of the ruling made against Fashion ID at first instance.

Fashion ID argues before the referring court that the decision of the Landgericht Düsseldorf (Regional Court, Düsseldorf) is incompatible with Directive 95/46.

First, Fashion ID claims that Articles 22 to 24 of that directive envisage granting legal remedies only to data subjects whose personal data are processed and the competent supervising authorities. Consequently, it argues, the action brought by Verbraucherzentrale NRW is inadmissible due to the fact that that association does not have standing to bring or defend legal proceedings under Directive 95/46.

Second, Fashion ID asserts that the Landgericht Düsseldorf (Regional Court, Düsseldorf) erred in finding that it was a controller, within the meaning of Article 2(d) of Directive 95/46, since it has no influence either over the data transmitted by the visitor's browser from its website or over whether and, where applicable, how Facebook Ireland uses those data.

In the first place, the referring court has doubts whether Directive 95/46 gives public-service associations the right to bring or defend legal proceedings in order to defend the interests of persons who have suffered harm. It takes the view that Article 24 of that directive does not preclude associations from being a party to

legal proceedings, since, pursuant to that article, Member States are required to adopt 'suitable measures' to ensure the full implementation of that directive. Thus, the referring court concludes that national legislation allowing associations to bring legal proceedings in the interest of consumers may constitute such a 'suitable measure'.

That court notes, in this regard, that Article 80(2) of Regulation 2016/679, which repealed and replaced Directive 95/46, expressly authorises the bringing of legal proceedings by such an association, which would tend to confirm that the latter directive did not preclude such an action.

Further, that court is uncertain whether the operator of a website, such as Fashion ID, that embeds on that website a social plugin allowing personal data to be collected can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46 despite the latter having no control over the processing of the data transmitted to the provider of that plugin. In this context, the referring court refers to the case that gave rise to the judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), which dealt with a similar question.

In the alternative, in the event that Fashion ID is not to be considered to be a controller, the referring court is uncertain whether that directive exhaustively regulates that notion, such that it precludes national legislation that establishes civil liability for a third party who infringes data protection rights. The referring court asserts that it would be possible to envisage Fashion ID being liable on this basis under national law as a 'disrupter' ('Störer').

If Fashion ID had to be considered to be a controller or was at least liable as a 'disrupter' for any data protection infringements by Facebook Ireland, the referring court is uncertain whether the processing of the personal data at issue in the main proceedings is lawful and whether the duty to inform the data subject under Article 10 of Directive 95/46 rests with Fashion ID or with Facebook Ireland.

Thus, first, with regard to the conditions for the lawfulness of the processing of data as provided for in Article 7(f) of Directive 95/46, the referring court expresses uncertainty as to whether, in a situation such as that at issue in the main proceedings, it is appropriate to take into account the legitimate interest of the operator of the website or that of the provider of the social plugin.

Second, that court is unsure who is required to obtain the consent of and inform the data subjects whose personal data are processed in a situation such as that at issue in the main proceedings. The referring court takes the view that the matter of who is obliged to inform the persons concerned, as provided for in Article 10 of Directive 95/46, is particularly important given that any embedding of third-party content on a website gives rise, in principle, to the processing of personal data, the scope and purpose of which are, however, unknown to the person embedding that content, namely the operator of the website concerned. That operator could not, therefore, provide the information required, to the extent that it is required to, meaning that the imposition of an obligation on the operator to inform the data subjects would, in practice, amount to a prohibition on the embedding of third-party content.

In those circumstances, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Do the rules in Articles 22, 23 and 24 of Directive [95/46] preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grants public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?

If Question 1 is answered in the negative:

(2) In a case such as the present one, in which someone has embedded a programming code in his website which causes the user's browser to request content from a third party and, to this end, transmits personal data to the third party, is the person embedding the content the "controller" within the meaning of Article 2(d) of Directive [95/46] if that person is himself unable to influence this data-processing operation?

[…]

(4) Whose "legitimate interests", in a situation such as the present one, are the decisive ones in the balancing of interests to be undertaken pursuant to Article 7(f) of Directive [95/46]? Is it the interests in embedding third-party content or the interests of the third party?

(5) To whom must the consent to be declared under Articles 7(a) and 2(h) of Directive [95/46] be given in a situation such as that in the present case?

(6) Does the duty to inform under Article 10 of Directive [95/46] also apply in a situation such as that in the present case to the operator of the website who has embedded the content of a third party and thus creates the cause for the processing of personal data by the third party?'

CJEU held:

By its first question the referring court asks, in essence, whether Articles 22 to 24 of Directive 95/46 must be interpreted as precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the laws protecting personal data.

[…]

Article 28(4) of Directive 95/46 provides that a supervisory authority is to hear claims lodged by an association representing a data subject, within the meaning of Article 2(a) of that directive, concerning the protection of his rights and freedoms in regard to the processing of personal data.

However, no provision of that directive obliges Member States to provide, or expressly empowers them to provide, in their national law that an association can represent a data subject in legal proceedings or commence legal proceedings on its own initiative against the person allegedly responsible for an infringement of the laws protecting personal data.

Nevertheless, it does not follow from the above that Directive 95/46 precludes national legislation allowing consumer-protection associations to bring or defend legal proceedings against the person allegedly responsible for such an infringement.

[…] one of the underlying objectives of Directive 95/46 is to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data (see, to that effect, judgments of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 53, and of 27 September 2017, Puškár, C-73/16, EU:C:2017:725, paragraph 38). Recital 10 of Directive 95/46 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection which they afford but must, on the contrary, seek to ensure a high level of protection in the European Union (judgments of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596, paragraph 95, of 16 December 2008, Huber, C-524/06, EU:C:2008:724, paragraph 50, and of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 and C-469/10, EU:C:2011:777, paragraph 28).

The fact that a Member State provides in its national legislation that it is possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives.

By its second question, the referring court asks, in essence, whether the operator of a website, such as Fashion ID, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46, despite that operator being unable to influence the processing of the data transmitted to

that provider as a result.

In this regard, it should be noted that, in accordance with the aim pursued by Directive 95/46, namely to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, Article 2(d) of that directive defines the concept of 'controller' broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (see, to that effect, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraphs 26 and 27).

As the Court has held previously, the objective of that provision is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects (judgments of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 34, and of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 28).

Furthermore, since, as Article 2(d) of Directive 95/46 expressly provides, the concept of 'controller' relates to the entity which 'alone or jointly with others' determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data-protection provisions (see, to that effect, judgments of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 29, and of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 65).

The Court has also held that a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46 (judgment of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 68).

Furthermore, the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, to that effect, judgments of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 38, and of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 69).

That said, since the objective of Article 2(d) of Directive 95/46 is to ensure, through a broad definition of the concept of 'controller', the effective and comprehensive protection of the persons concerned, the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case (see, to that effect, judgment of 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, paragraph 66).

[…] the processing of personal data may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve.

[…] where several operators determine jointly the purposes and means of the processing of personal data, they participate in that processing as controllers.

[…] a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means.

[…] the operations involving the processing of personal data in respect of which Fashion ID is capable of determining, jointly with Facebook Ireland, the purposes and means are, for the purposes of the definition of the concept of 'processing of personal data' in Article 2(b) of Directive 95/46, the collection and disclosure by transmission of the personal data of visitors to its website. By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means

of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).

With regard to the means used for the purposes of the collection and disclosure by transmission of certain personal data of visitors to its website, it is apparent […] that Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook.

Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin.

[…] Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website.

As to the purposes of those operations involving the processing of personal data, it appears that Fashion ID's embedding of the Facebook 'Like' button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID.

In such circumstances, it can be concluded […] that Fashion ID and Facebook Ireland determine jointly the purposes of the operations involving the collection and disclosure by transmission of the personal data at issue in the main proceedings.

[…] the fact that the operator of a website, such as Fashion ID, does not itself have access to the personal data collected and transmitted to the provider of the social plugin with which it determines jointly the means and purposes of the processing of personal data does not preclude it from being a controller within the meaning of Article 2(d) of Directive 95/46.\

[…] a website, such as that of Fashion ID, is visited both by those who are members of the social network Facebook, and who therefore have an account on that social network, and by those who do not have one. In that latter case, the responsibility of the operator of a website, such as Fashion ID, for the processing of the personal data of those persons appears to be even greater, as the mere consultation of such a website featuring the Facebook 'Like' button appears to trigger the processing of their personal data by Facebook Ireland (see, to that effect. judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 41).

Accordingly, it seems that Fashion ID can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46, jointly with Facebook Ireland, in respect of the operations involving the collection and disclosure by transmission of the personal data of visitors to its website.

By its fourth question, the referring court asks, in essence, whether, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is appropriate, for the purposes of the application of Article 7(f) of Directive 95/46, to take into consideration a legitimate interest pursued by that operator or a legitimate interest pursued by that provider.

[…] it should be noted at the outset that, according to the provisions of Chapter II of Directive 95/46, headed 'General rules on the lawfulness of the processing of personal data', subject to the derogations

permitted under Article 13 of that directive, all processing of personal data must comply, inter alia, with one of the criteria for making data processing legitimate listed in Article 7 of that directive (see, to that effect, judgments of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 71, and of 1 October 2015, Bara and Others, C-201/14, EU:C:2015:638, paragraph 30).

Under Article 7(f) of Directive 95/46, the interpretation of which is sought by the referring court, personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1) of Directive 95/46.

Article 7(f) of that directive thus lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence (judgment of 4 May 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, paragraph 28).

Given that, in the light of the answer to the second question, it seems that, in a situation such as that at issue in the main proceedings, the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller responsible, jointly with that provider, for operations involving the processing of the personal data of visitors to its website in the form of collection and disclosure by transmission, it is necessary that each of those controllers should pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them.

By its fifth and sixth questions, which it is appropriate to examine together, the referring court wishes to know, in essence, first, whether Articles 2(h) and 7(a) of Directive 95/46 must be interpreted as meaning that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator or by that provider and, second, whether Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform provided for in that provision is incumbent on that operator.

As is apparent from the answer to the second question, the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46, despite that liability being limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means.

It thus appears that the duties that may be incumbent on that controller under Directive 95/46, such as the duty to obtain the consent of the data subject under Articles 2(h) and 7(a) of that directive and the duty to inform under Article 10 thereof, must relate to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means.

In the present case, while the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, jointly with that provider, in respect of operations involving the collection and disclosure by transmission of the personal data of that visitor, its duty to obtain the consent from the data subject under Articles 2(h) and 7(a) of Directive 95/46 and its duty to inform under Article 10 of that directive relate only to those operations. By contrast, those duties do not cover operations involving the processing of personal data at other stages occurring before or after those operations which involve, as the case may be, the processing of personal data at issue.

With regard to the consent referred to in Articles 2(h) and 7(a) of Directive 95/46, it appears that such consent must be given prior to the collection and disclosure by transmission of the data subject's data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data. As the Advocate General noted in point 132 of his Opinion, it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.

The same applies in regard to the duty to inform under Article 10 of Directive 95/46.

In that regard, it follows from the wording of that provision that the controller or his representative must provide, as a minimum, the information referred to in that provision to the subject whose data are being collected. It thus appears that that information must be given by the controller immediately, that is to say, when the data are collected (see, to that effect, judgments of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293, paragraph 68, and of 7 November 2013, IPI, C-473/12, EU:C:2013:715, paragraph 23).

It follows that, in a situation such as that at issue in the main proceedings, the duty to inform under Article 10 of Directive 95/46 is incumbent also on the operator of the website, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means.

On those grounds, the Court (Second Chamber) ruled:

"1. **Articles 22 to 24 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.**

2. **The operator of a website, such as Fashion ID GmbH & Co. KG, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue.**

3. **In a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them.**

4. **Articles 2(h) and 7(a) of Directive 95/46 must be interpreted as meaning that, in a situation such as that at issue in the main proceedings, in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator only**

with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means. In addition, Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform laid down in that provision is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means."

3. INTERNATIONAL TRANSFERS

3.1. C-362/14 (Schrems) (ECLI:EU:C:2015:650)

(Requests for a preliminary ruling from the High Court (Ireland))

(Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities)

Judgment of the Court (Grand Chamber), 6 October 2015

THE QUESTIONS:

Mr Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

On 25 June 2013 Mr Schrems made a complaint to the Commissioner by which he in essence asked the latter to exercise his statutory powers by prohibiting Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA').

Since the Commissioner took the view that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected it as unfounded. The Commissioner considered that there was no evidence that Mr Schrems' personal data had been accessed by the NSA. He added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection.

Mr Schrems brought an action before the High Court challenging the decision at issue in the main proceedings. After considering the evidence adduced by the parties to the main proceedings, the High Court

found that the electronic surveillance and interception of personal data transferred from the European Union to the United States serve necessary and indispensable objectives in the public interest. However, it added that the revelations made by Edward Snowden had demonstrated a 'significant over-reach' on the part of the NSA and other federal agencies.

According to the High Court, Union citizens have no effective right to be heard. Oversight of the intelligence services' actions is carried out within the framework of an ex parte and secret procedure. Once the personal data has been transferred to the United States, it is capable of being accessed by the NSA and other federal agencies, such as the Federal Bureau of Investigation (FBI), in the course of the indiscriminate surveillance and interception carried out by them on a large scale.

The High Court stated that Irish law precludes the transfer of personal data outside national territory save where the third country ensures an adequate level of protection for privacy and fundamental rights and freedoms. The importance of the rights to privacy and to inviolability of the dwelling, which are guaranteed by the Irish Constitution, requires that any interference with those rights be proportionate and in accordance with the law.

The High Court held that the mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution. In order for interception of electronic communications to be regarded as consistent with the Irish Constitution, it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime and that there are appropriate and verifiable safeguards. Thus, according to the High Court, if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the United States ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matters raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint.

However, the High Court considers that this case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter and from the principles set out by the Court of Justice in the judgment in Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238). The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.

The High Court further observes that in his action Mr Schrems in reality raises the legality of the safe harbour regime which was established by Decision 2000/520 and gives rise to the decision at issue in the main proceedings. Thus, even though Mr Schrems has not formally contested the validity of either Directive 95/46 or Decision 2000/520, the question is raised, according to the High Court, as to whether, on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520 that the United States ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding.

In those circumstances the High Court decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?'

CJEU held:

"By its questions, which it is appropriate to examine together, the referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

[…]

As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU (see, to this effect, judgments in Commission v Austria, C-614/10, EU:C:2012:631, paragraph 36, and Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 47).

The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data (see judgments in Commission v Germany, C-518/07, EU:C:2010:125, paragraph 25, and Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 48 and the case-law cited).

In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data (see, to this effect, judgments in Commission v Germany, C-518/07, EU:C:2010:125, paragraph 24, and Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 51).

The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings.

It is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so that they do not have powers on the basis of Article 28 in respect of processing of such data carried out in a third country.

However, the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive

95/46 (see, to this effect, judgment in Parliament v Council and Commission, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'.

Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data (see, to this effect, judgment in Lindqvist, C-101/01, EU:C:2003:596, paragraph 63).

As, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

[…] transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited.

[…]

The Commission may adopt, on the basis of Article 25(6) of Directive 95/46, a decision finding that a third country ensures an adequate level of protection. In accordance with the second subparagraph of that provision, such a decision is addressed to the Member States, who must take the measures necessary to comply with it. Pursuant to the fourth paragraph of Article 288 TFEU, it is binding on all the Member States to which it is addressed and is therefore binding on all their organs (see, to this effect, judgments in Albako Margarinefabrik, 249/85, EU:C:1987:245, paragraph 17, and Mediaset, C-69/13, EU:C:2014:71, paragraph 23) in so far as it has the effect of authorising transfers of personal data from the Member States to the third country covered by it.

Thus, until such time as the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in Commission v Greece, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited).

However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim, within the meaning of Article 28(4) of that directive, concerning the protection of their rights and freedoms in regard to the processing of that data. Likewise, as the Advocate General has observed in particular in points 61, 93 and 116 of his Opinion, a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive.

Neither Article 8(3) of the Charter nor Article 28 of Directive 95/46 excludes from the national supervisory authorities' sphere of competence the oversight of transfers of personal data to third countries which have been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46.

In particular, the first subparagraph of Article 28(4) of Directive 95/46, under which the national supervisory authorities are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive.

[…] Thus, even if the Commission has adopted a decision pursuant to Article 25(6) of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.

[…] the Court alone has jurisdiction to declare that an EU act, such as a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (see judgments in Melki and Abdeli, C-188/10 and C-189/10, EU:C:2010:363, paragraph 54, and CIVAD, C-533/10, EU:C:2012:347, paragraph 40).

[…] where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence.

In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must, as is apparent from the second subparagraph of Article 28(3) of Directive 95/46, read in the light of Article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Having regard to the case-law cited in paragraphs 61 and 62 of the present judgment, those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (see, to this effect, judgment in T & L Sugars and Sidul Açúcares v Commission, C-456/13 P, EU:C:2015:284, paragraph 48 and the case-law cited).

In the converse situation, where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, that authority must, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, be able to engage in legal proceedings. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.

The validity of Decision 2000/520

As is apparent from the referring court's explanations relating to the questions submitted, Mr Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. As the Advocate General has observed in points 123 and 124 of his Opinion, Mr Schrems expresses doubts, which the referring court indeed seems essentially to share, concerning the validity of Decision 2000/520. In such circumstances, having regard to what has been held in paragraphs 60 to 63 of the present judgment and in order to give the referring court a full answer, it should be examined whether that decision complies with the requirements stemming from Directive 95/46 read in the light of the Charter.

[…] neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on

a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals.

Thus, Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.

The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.

It is clear from the express wording of Article 25(6) of Directive 95/46 that it is the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union.

Article 1 of Decision 2000/520

The Commission found in Article 1(1) of Decision 2000/520 that the principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those principles and the FAQs were issued by the United States Department of Commerce.

An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto.

Whilst recourse by a third country to a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice.

In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are 'intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of "adequacy" it creates'. Those

principles are therefore applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them.

Moreover, Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments.

In addition, under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'.

In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, '[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'.

Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.

In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited).

In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.

Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, procedures before the Federal Trade Commission — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms concern compliance by the United States undertakings with the safe harbour principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.

Moreover, […] the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing

the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in Les Verts v Parliament, 294/83, EU:C:1986:166, paragraph 23; Johnston, 222/84, EU:C:1986:206, paragraphs 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, paragraph 14; and UGT-Rioja and Others, C-428/06 to C-434/06, EU:C:2008:488, paragraph 80).

Article 3 of Decision 2000/520

[…] the first subparagraph of Article 3(1) of Decision 2000/520 lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection, within the meaning of Article 25 of Directive 95/46.

Under that provision, the national supervisory authorities may, '[w]ithout prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive [95/46], … suspend data flows to an organisation that has self-certified its adherence to the [principles of Decision 2000/520]', under restrictive conditions establishing a high threshold for intervention. Whilst that provision is without prejudice to the powers of those authorities to take action to ensure compliance with national provisions adopted pursuant to Directive 95/46, it excludes, on the other hand, the possibility of them taking action to ensure compliance with Article 25 of that directive.

The first subparagraph of Article 3(1) of Decision 2000/520 must therefore be understood as denying the

national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person, in bringing a claim under that provision, puts forward matters that may call into question whether a Commission decision that has found, on the basis of Article 25(6) of the directive, that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.

The implementing power granted by the EU legislature to the Commission in Article 25(6) of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers referred to in the previous paragraph of the present judgment.

[…]

As Articles 1 and 3 of Decision 2000/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety."

On those grounds, the Court (Grand Chamber) ruled:

1. **Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**

2. **Decision 2000/520 is invalid.**

3.2. Opinion 1/15 of the Court (Grand Chamber) on the Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (ECLI:EU:C:2017:592)

The European Parliament requested the Court for an opinion:

"Is the [envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data] compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to the protection of personal data?"

The Court issued the following opinion:

"The Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data is incompatible with Articles 7, 8 and 21 and Article 52(1) of the Charter of Fundamental Rights of the European Union in so far as it does not preclude the transfer of sensitive data from the European Union to Canada and the use and retention of that data.

The Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data must, in order to be compatible with Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights:

(a) determine in a clear and precise manner the PNR data to be transferred from the European Union to Canada;

(b) provide that the models and criteria used in the context of automated processing of PNR data will be specific and reliable and non-discriminatory; provide that the databases used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;

(c) save in the context of verifications in relation to the pre-established models and criteria on which automated processing of Passenger Name Record data is based, make the use of that data by the Canadian Competent Authority during the air passengers' stay in Canada and after their departure from that country, and any disclosure of that data to other authorities, subject to substantive and procedural conditions based on objective criteria; make that use and that disclosure, except in cases of validly established urgency, subject to a prior review carried out either by a court or by an independent administrative body, the decision of that court or body authorising the use being made following a reasoned request by those authorities, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime;

(d) limit the retention of Passenger Name Record data after the air passengers' departure to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime;

(e) make the disclosure of Passenger Name Record data by the Canadian Competent Authority to the government authorities of a third country subject to the condition that there be either an agreement between the European Union and that third country equivalent to the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, or a decision of the European Commission, under Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, covering the authorities to which it is intended that Passenger Name Record data be disclosed;

(f) provide for a right to individual notification for air passengers in the event of use of Passenger Name Record data concerning them during their stay in Canada and after their departure from that country, and in the event of disclosure of that data by the Canadian Competent Authority to other authorities or to individuals; and

(g) guarantee that the oversight of the rules laid down in the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data relating to the protection of air passengers with regard to the processing of Passenger Name Record data concerning them will be carried out by an independent supervisory authority."

4. THE RIGHT TO BE FORGOTTEN

4.1. C-131/12 (Google Spain and Google) (ECLI:EU:C:2014:317)

(Requests for a preliminary ruling from the Audiencia Nacional (Spain))

(Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

Judgment of the Court (Grand Chamber), 13 May 2014

THE QUESTIONS:

On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD [the Spanish Data Protection National Authority - Agencia Española de Protección de Datos] a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional joined the actions.

That court states in the order for reference that the actions raise the question of what obligations are owed

by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive's publication.

In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:

(a) Must it be considered that an "establishment", within the meaning of Article 4(1)(a) of Directive 95/46, exists when any one or more of the following circumstances arise:

- when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,

  or

- when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,

  or

- when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

(b) Must Article 4(1)(c) of Directive 95/46 be interpreted as meaning that there is "use of equipment … situated on the territory of the said Member State":

- when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,

  or

- when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?

(c) Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?

(d) Regardless of the answers to the foregoing questions and particularly in the event that the Court … considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present: must Directive 95/46 … be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of … Union citizens is possible?

2. As regards the activity of search engines as providers of content in relation to Directive 95/46 …:

(a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of

preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of Directive 95/46?

(b) If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described: must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the "controller" of the personal data contained in the web pages that it indexes?

(c) In the event that the answer to the foregoing question is affirmative: may the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d) In the event that the answer to the foregoing question is affirmative: would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked: must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?""

CJUE held:

"By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

[…]

Article 2(b) of Directive 95/46 defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 Lindqvist EU:C:2003:596, paragraph 25).

So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of

that directive.

Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

The Court has already held that the operations referred to in Article 2(b) of Directive 95/46 must also be classified as such processing where they exclusively concern material that has already been published in unaltered form in the media. It has indeed observed in that regard that a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect (see, to this effect, Case C-73/07 Satakunnan Markkinapörssi and Satamedia EU:C:2008:727, paragraphs 48 and 49).

Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.

As to the question whether the operator of a search engine must be regarded as the 'controller' in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 defines 'controller' as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.

It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.

In this connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.

Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.

Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive

may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.

Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive', that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

That fact does not alter the position that the purposes and means of that processing are determined by the operator of the search engine. Furthermore, even if that option for publishers of websites were to mean that they determine the means of that processing jointly with that operator, this finding would not remove any of the latter's responsibility as Article 2(d) of Directive 95/46 expressly provides that that determination may be made 'alone or jointly with others'.

By Question 1(a) to (d), the referring court seeks to establish whether it is possible to apply the national legislation transposing Directive 95/46 in circumstances such as those at issue in the main proceedings.

In this respect, the referring court has established the following facts:

– Google Search is offered worldwide through the website 'www.google.com'. In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website 'www.google.es', which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.

– Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.

– Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its 'web crawlers' or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.

– Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users.

– The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com'. Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain). Its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group in that Member State. Its objectives are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.

– Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.

Specifically, the main issues raised by the referring court concern the notion of 'establishment', within the meaning of Article 4(1)(a) of Directive 95/46, and of 'use of equipment situated on the territory of the said Member State', within the meaning of Article 4(1)(c).

[…]

In this regard, it is to be noted first of all that recital 19 in the preamble to Directive 95/46 states that 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements' and that 'the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor'.

It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46.

In order to satisfy the criterion laid down in that provision, it is also necessary that the processing of personal data by the controller be 'carried out in the context of the activities' of an establishment of the controller on the territory of a Member State.

[…]

It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

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.

In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

[…] [T]he very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure (see, by analogy, L'Oréal and Others EU:C:2011:474, paragraphs 62 and 63), in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance as is confirmed in particular by Article 1(1) thereof and recitals 2 and 10 in its preamble (see, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 70; Case C-553/07 Rijkeboer EU:C:2009:293, paragraph 47; and Case C-473/12 IPI EU:C:2013:715, paragraph 28 and the case-law cited).

By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see, to this effect, IPI EU:C:2013:715, paragraph 28).

According to recital 25 in the preamble to Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P Connolly v Commission EU:C:2001:127, paragraph 37, and Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 68).

Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.

Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data.

In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 ASNEF and FECEMD EU:C:2011:777, paragraph 26; and Case C-342/12 Worten EU:C:2013:355, paragraph 33).

Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.

As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).

This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a

balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (see ASNEF and FECEMD, EU:C:2011:777, paragraphs 38 and 40).

Whilst the question whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the directive, the data subject may, in addition, rely in certain conditions on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the directive.

Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

In this connection, it is to be noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.

[…] [The] processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45).

In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

Following the appraisal of the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 which is to be carried out when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on

the basis of a person's name links to web pages published by third parties containing information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published.

[…] [I]nasmuch as the data processing carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites and affects the data subject's fundamental rights additionally, the operator of the search engine as the controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect.

Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.

Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.

Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.

Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

[…]

As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, it should be recalled that, as has been noted in paragraph 72 of the present judgment, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially

lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

So far as concerns requests as provided for by Article 12(b) of Directive 95/46 founded on alleged non-compliance with the conditions laid down in Article 7(f) of the directive and requests under subparagraph (a) of the first paragraph of Article 14 of the directive, it must be pointed out that in each case the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out.

In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.

As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.

It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those

rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."

On those grounds, the Court (Grand Chamber) ruled:

"1. Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

2. Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

3. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

4. Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question."

4.2. C-553/07 (Rijkeboer) (ECLI:EU:C:2009:293)

(Requests for a preliminary ruling from Raad van State (Netherlands))

(Protection of individuals with regard to the processing of personal data – Directive 95/46/EC – Respect for private life – Erasure of data – Right of access to data and to information on the recipients of data – Time-limit on the exercise of the right to access)

Judgment of the Court (Third Chamber), 7 May 2009

THE QUESTION:

"By letter of 26 October 2005, Mr Rijkeboer requested the College [van burgemeester en wethouders van Rotterdam - Board of Aldermen of Rotterdam] to notify him of all instances in which data relating to him from the local authority personal records had, in the two years preceding the request, been disclosed to third parties. He wished to know the identity of those persons and the content of the data disclosed to them. Mr Rijkeboer, who had moved to another municipality, wished to know in particular to whom his former address had been disclosed.

By decisions of 27 October and 29 November 2005, the College complied with that request only in part by notifying him only of the data relating to the period of one year preceding his request, by application of Article 103(1) of the Wet GBA [The Law on personal data held by local authorities (Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, No 494; 'the Wet GBA').].

Communication of the data is registered and stored in electronic form in accordance with the 'Logisch Ontwerp GBA' (GBA Logistical Project). This is an automated system established by the Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (Netherlands Ministry of the Interior and Home Affairs). It is apparent from the reference for a preliminary ruling that the data requested by Mr Rijkeboer dating from more than one year prior to his request were automatically erased, which accords with the provisions of Article 110 of the Wet GBA.

Mr Rijkeboer lodged a complaint with the College against the refusal to give him the information relating to the recipients to whom data regarding him had been disclosed during the period before the year preceding his request. That complaint having been rejected by decision of 13 February 2006, Mr Rijkeboer brought an action before the Rechtbank Rotterdam.

That court upheld the action, taking the view that the restriction on the right to information on provision of data to the year before the request, as provided for in Article 103(1) of the Wet GBA, is at variance with Article 12 of the Directive. It also held that the exceptions referred to in Article 13 of that directive are not applicable.

The College appealed against that decision to the Raad van State. That court finds that Article 12 of the Directive on rights of access to data does not indicate any time period within which it must be possible for those rights to be exercised. In its view, that article does not necessarily, however, preclude Member States from imposing a time restriction in their national legislation on the data subject's right to information concerning the recipients to whom personal data have been provided, but the court has doubts in that regard.

In those circumstances the Raad van State decided to stay the proceedings and to refer the following question to the Court for a preliminary ruling:

'Is the restriction, provided for in the [Netherlands] Law [on local authority personal records], on the communication of data to one year prior to the relevant request compatible with Article 12(a) of [the] Directive …, whether or not read in conjunction with Article 6(1)(e) of that directive and the principle of proportionality?'

CJEU held:

[…] the question referred by the national court should be understood, essentially, as seeking to determine whether, pursuant to the Directive and, in particular, to Article 12(a) thereof, an individual's right of access to information on the recipients or categories of recipients of personal data regarding him and on the content of the data communicated may be limited to a period of one year preceding his request for access.

[…]

Article 6 of the Directive deals with the quality of the data. Article 6(1)(e) requires Member States to ensure that personal data are kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The data must therefore be erased when those purposes have been served.

Article 12(a) of the Directive provides that Member States are to guarantee data subjects a right of access to their personal data and to information on the recipients or categories of recipient of those data, without setting a time-limit.

In order to assess the scope of the right of access which the Directive must make possible, it is appropriate, first, to determine what data are covered by the right of access and, next, to turn to the objective of Article 12(a) examined in the light of the purposes of the Directive.

A case such as that of Mr Rijkeboer involves two categories of data.

The first concerns personal data kept by the local authority on a person, such as his name and address, which constitute, in the present case, the basic data. It is apparent from the oral observations submitted by the College and the Netherlands Government that those data may be stored for a long time. They constitute 'personal data' within the meaning of Article 2(a) of the Directive, because they represent information relating to an identified or identifiable natural person (see, to that effect, Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989, paragraph 64; Case C-101/01 Lindqvist [2003] ECR I-12971, paragraph 24; and Case C-524/06 Huber [2008] ECR I-0000, paragraph 43).

The second category concerns information on recipients or categories of recipient to whom those basic data are disclosed and on the content thereof and thus relates to the processing of the basic data. In accordance with the national legislation at issue in the main proceedings, that information is stored for only one year.

The time-limit on the right of access to information on the recipient or recipients of personal data and on the content of the data disclosed, which is referred to in the main proceedings, thus concerns that second category of data.

In order to determine whether or not Article 12(a) of the Directive authorises such a time-limit, it is appropriate to interpret that article having regard to its objective examined in the light of the purposes of the Directive.

[…]

[The] right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. As is stated in recital 41 in the preamble to the Directive, in order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed.

In that regard, Article 12(a) of the Directive provides for a right of access to basic data and to information on the recipients or categories of recipient to whom the data are disclosed.

That right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of the Directive, that is to say, where the processing of his data does not comply with the provisions of the Directive, the right to have the controller rectify, erase or block his data, (paragraph (b)), or notify

third parties to whom the data have been disclosed of that rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort (paragraph (c)).

That right of access is also necessary to enable the data subject to exercise his right referred to in Article 14 of the Directive to object to his personal data being processed or his right of action where he suffers damage, laid down in Articles 22 and 23 thereof.

With regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed, the Directive does not make it clear whether that right concerns the past and, if so, what period in the past.

In that regard, to ensure the practical effect of the provisions referred to in paragraphs 51 and 52 of the present judgment, that right must of necessity relate to the past. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered.

A question arises as to the scope of that right in the past.

The Court has already held that the provisions of the Directive are necessarily relatively general since it has to be applied to a large number of very different situations and that the Directive includes rules with a degree of flexibility, in many instances leaving to the Member States the task of deciding the details or choosing between options (see Lindqvist, paragraph 83). Thus, the Court has recognised that, in many respects, the Member States have some freedom of action in implementing the Directive (see Lindqvist, paragraph 84). That freedom, which becomes apparent with regard to the transposition of Article 12(a) of the Directive, is not, however, unlimited.

The setting of a time-limit with regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed must allow the data subject to exercise the different rights laid down in the Directive and referred to in paragraphs 51 and 52 of the present judgment.

The length of time the basic data are to be stored may constitute a useful parameter without, however, being decisive.

The scope of the Directive is very wide, as the Court has already held (see Österreichischer Rundfunk and Others, paragraph 43, and Lindqvist, paragraph 88), and the personal data covered by the Directive are varied. The length of time such data are to be stored, defined in Article 6(1)(e) of the Directive according to the purposes for which the data were collected or for which they are further processed, can therefore differ. Where the length of time for which basic data are to be stored is very long, the data subject's interest in exercising the rights to object and to remedies referred to in paragraph 57 of the present judgment may diminish in certain cases. If, for example, the relevant recipients are numerous or there is a high frequency of disclosure to a more restricted number of recipients, the obligation to keep the information on the recipients or categories of recipient of personal data and on the content of the data disclosed for such a long period could represent an excessive burden on the controller.

The Directive does not require Member States to impose such burdens on the controller.

Accordingly, Article 12(c) of the Directive expressly provides for an exception to the obligation on the controller to notify third parties to whom the data have been disclosed of any correction, erasure or blocking, namely, where this proves impossible or involves a disproportionate effort.

In accordance with other sections of the Directive, account may be taken of the disproportionate nature of other possible measures. With regard to the obligation to inform the data subject, recital 40 in the preamble to the Directive states that the number of data subjects and the age of the data may be taken into consideration. Furthermore, in accordance with Article 17 of the Directive concerning security of processing, Member States are to provide that the controller must implement appropriate technical and organisational measures which, having regard to the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Analogous considerations are relevant with regard to the fixing of a time-limit on the right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed. In addition to the considerations referred to in paragraph 57 of the present judgment, a number of parameters may accordingly be taken into account by the Member States, in particular applicable provisions of national law on time-limits for bringing an action, the more or less sensitive nature of the basic data, the length of time for which those data are to be stored and the number of recipients.

Thus it is for the Member States to fix a time-limit for storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to rectification, erasure and blocking of the data in the event that the processing of the data does not comply with the Directive, and rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.

Moreover, when fixing that time-limit, it is appropriate to take account also of the obligations which following from Article 6(e) of the Directive to ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

In the present case, rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the verifications necessary in the light of the considerations set out in the preceding paragraphs.

Having regard to the foregoing considerations, the argument of some Member States that application of Articles 10 and 11 of the Directive renders superfluous a grant in respect of the past of a right to access to information on the recipients or categories of recipient referred to in Article 12(a) of the Directive cannot be accepted.

Articles 10 and 11 impose obligations on the controller or his representative to inform the data subject, in certain circumstances, in particular of the recipients or categories of recipient of the data. The controller or his representative must communicate that information to the data subject of their own accord, inter alia when the data are collected or, if the data are not collected directly from the data subject, when the data are registered or, possibly, when the data are disclosed to a third party.

In that way, those provisions are intended to impose obligations distinct from those which follow from Article 12(a) of the Directive. Consequently, they in no way reduce the obligation placed on Member States to ensure that the controller is required to give a data subject access to the information on the recipients or categories of recipient and on the data disclosed when that data subject decides to exercise his right to access conferred on him by Article 12(a). Member States must adopt measures transposing, firstly, the provisions of Articles 10 and 11 of the Directive on the obligation to provide information and, secondly, those of Article 12(a) of the Directive, without it being possible for the former to attenuate the obligations following from the latter."

On those grounds, the Court (Third Chamber) ruled:

"Article 12(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a

fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.

Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary."

4.3. C-398/15 (Manni) (ECLI:EU:C:2017:197)

(Requests for a preliminary ruling from the Corte suprema di cassazione (Italy))

(Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Article 6(1)(e) — Data subject to disclosure in the companies register — First Directive 68/151/EEC — Article 3 — Winding-up of the company concerned — Restriction of access to that data by third parties)

Judgment of the Court (Second Chamber), 9 March 2017

THE QUESTION:

Mr Manni is the sole director of Italiana Costruzioni Srl, a building company which was awarded a contract for the construction of a tourist complex.

By an action commenced on 12 December 2007, Mr Manni brought proceedings against the Lecce Chamber of Commerce, claiming that the properties in that complex were not selling because it was apparent from the companies register that he had been the sole director and liquidator of Immobiliare e Finanziaria Salentina Srl ('Immobiliare Salentina'), which had been declared insolvent in 1992 and struck off the companies register, following liquidation proceedings, on 7 July 2005.

In that action, Mr Manni alleged that the personal data concerning him, which appear in the companies register, had been processed by a company specialised in the collection and processing of market information and in risk assessment ('rating'), and that, notwithstanding a request to remove it from the register, the Lecce Chamber of Commerce has not done so.

Mr Manni therefore sought an order requiring the Lecce Chamber of Commerce to erase, anonymise or block the data linking him to the liquidation of Immobiliare Salentina, together with an order that that chamber compensate him for the damage he suffered by reason of the injury to his reputation.

By judgment of 1 August 2011, the Tribunale di Lecce (Court of Lecce, Italy) upheld that claim, ordering the Lecce Chamber of Commerce to anonymise the data linking Mr Manni to the liquidation of Immobiliare Salentina and to pay compensation for the damage suffered by him, assessed at EUR 2 000, together with interest and costs.

The Tribunale di Lecce (Court of Lecce) considered that 'it is not permissible for entries in the register which link the name of an individual to a critical phase in the life of the company (such as its liquidation) to be permanent, unless there is a specific general interest in their retention and disclosure'. In the absence of any provision in the Civil Code laying down a maximum period of registration, that court held that, 'after an appropriate period' from the conclusion of the liquidation, and after the company has been removed from the register, stating the name of the person who was sole director of that company at the time of the liquidation ceased to be necessary and useful, for the purposes of Legislative Decree No 196, and the public interest in a 'historical memory' of the existence of the company and the difficulties it experienced

[could] to a great extent be just as well effected by means of anonymous data'.

The Lecce Chamber of Commerce brought an appeal against that judgment before the Corte suprema di cassazione (Court of Cassation, Italy), which decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Must the principle of keeping personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, laid down in Article 6(1)(e) of Directive 95/46, transposed by Legislative Decree No 196 of 30 June 2003, take precedence over and, therefore, preclude the system of disclosure established by means of the companies register provided for by Directive 68/151 and by national law in Article 2188 of the Civil Code and Article 8 of Law No 580 of 29 December 1993, in so far as it is a requirement of that system that anyone may, at any time, obtain the data relating to individuals in those registers?

(2) Consequently, is it permissible under Article 3 of Directive 68/151, by way of derogation from the principles that there should be no time limit and that anyone may consult the data published in the companies register, for the data no longer to be subject to "disclosure", in both those regards, but to be available for only a limited period and only to certain recipients, on the basis of a case-by-case assessment by the data manager?'

CJEU held:

By its questions, which should be considered together, the referring court asks, essentially, whether Article 3 of Directive 68/151 and Article 6(1)(e) of Directive 95/46 must be interpreted as meaning that Member States may, and indeed must, allow individuals, covered by Article 2(1)(d) and (j) of Directive 68/151, to request the authority responsible for maintaining the companies register to limit, after a certain period has elapsed from the dissolution of the company concerned and on the basis of a case-by-case assessment, access to personal data concerning them and entered in that register.

[…] [I]t must first be pointed out that, under Article 2(1)(d) of Directive 68/151, Member States must take the measures necessary to ensure compulsory disclosure by companies of at least the appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law, or as members of any such body, are authorised to represent the company in dealings with third parties and in legal proceedings, or take part in the administration, supervision or control of that company. Moreover, according to Article 2(1)(j), the appointment of liquidators, particulars concerning them and, in principle, their respective powers must also be disclosed.

Pursuant to Article 3(1) to (3) of Directive 68/151, those particulars must be transcribed in each Member State either in a central register, commercial register or companies register (together, 'the register'), and a copy of the whole or any part of those particulars must be obtainable by application.

It must be held that the particulars concerning the identity of the persons referred to in Article 2(1)(d) and (j) of Directive 68/151 constitute, as information relating to identified or identifiable natural persons, 'personal data' within the meaning of Article 2(a) of Directive 95/46. It is apparent from the Court's case-law that the fact that that information was provided as part of a professional activity does not mean that it cannot be characterised as personal data (see judgment of 16 July 2015, ClientEarth and PAN Europe v EFSA, C-615/13 P, EU:C:2015:489, paragraph 30 and the case-law cited).

Furthermore, by transcribing and keeping that information in the register and communicating it, where appropriate, on request to third parties, the authority responsible for maintaining that register carries out 'processing of personal data' for which it is the 'controller', within the meaning of the definitions set out Article 2(b) and (d) of Directive 95/46.

The processing of personal data which is thus carried out in the implementation of Article 2(1)(d) and

(j) and Article 3 of Directive 68/151 is subject to Directive 95/46, under Articles 1 and 3 thereof. This is now expressly provided for in Article 7a of Directive 2009/101, as amended by Directive 2012/17, which, however, is only declaratory in that regard. As the European Commission stated at the hearing, the EU legislature considered it useful to recall that fact in the context of the legislative changes introduced by Directive 2012/17 and aimed at ensuring interoperability of registers of the Member States, since those changes suggested an increase in the intensity of the processing of personal data.

With regard to Directive 95/46, it should be remembered that, as is apparent from Article 1 and recital 10, that directive seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see judgment of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 66 and the case-law cited).

According to recital 25 of Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing data, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that such processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms and, in particular, the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union ('the Charter') (see judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 38 and the case-law cited).

Article 7 of the Charter therefore guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) states that such data must be processed fairly, for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified, and that compliance with those rules is to be subject to control by an independent authority. Those requirements are implemented inter alia in Articles 6, 7, 12, 14 and 28 of Directive 95/46.

With regard, in particular, to the general conditions of lawfulness imposed by Directive 95/46, it should be noted that, subject to the exceptions permitted under Article 13 of that directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see, inter alia, judgment of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 71 and the case-law cited).

In that regard, as the Advocate General pointed out in point 52 of his Opinion, it should be noted that the processing of personal data by the authority responsible for keeping the register pursuant to Article 2(1)(d) and (j) and Article 3 of Directive 68/151 satisfies several grounds for legitimation provided for in Article 7 of Directive 95/46, namely those set out in subparagraph (c) thereof, relating to compliance with a legal obligation, subparagraph (e), relating to the exercise of official authority or the performance of a task carried out in the public interest, and subparagraph (f) relating to the realisation of a legitimate interest pursued by the controller or by the third parties to whom the data are disclosed.

With regard, inter alia, to the ground for legitimation provided for in Article 7(e) of Directive 95/46, it should be noted that the Court of Justice has already held that the activity of a public authority consisting in the storing, in a database, of data which undertakings are obliged to report on the basis of statutory obligations, permitting interested persons to search for that data and providing them with print-outs thereof, falls within the exercise of public powers (see judgment of 12 July 2012, Compass-Datenbank, C-138/11, EU:C:2012:449, paragraphs 40 and 41). Moreover, such an activity also constitutes a task carried out in the public interest within the meaning of that provision.

In the present case, the parties to the main proceedings disagree as to whether the authority responsible for keeping the register should, after a certain period has elapsed since a company ceased to trade, and

on the request of the data subject, either erase or anonymise that personal data, or limit their disclosure. In that context, the referring court asks in particular whether such an obligation flows from Article 6(1)(e) of Directive 95/46.

According to Article 6(1)(e) of Directive 95/46, Member States are to ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Where that data are stored for longer periods for historical, statistical or scientific use, Member States must lay down appropriate safeguards. Pursuant to paragraph 2 of that article, it is the responsibility of the controller to ensure compliance with those principles.

In the event of failure to comply with the condition laid down in Article 6(1)(e) of Directive 95/46, Member States guarantee the person concerned, pursuant to Article 12(b) thereof, the right to obtain from the controller, as appropriate, the erasure or blocking of the data concerned (see, to that effect, judgment of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 70).

Moreover, under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, inter alia in the cases referred to in Article 7(e) and (f) of that directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data (see judgment of 13 May 2014, Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 76).

In order to determine whether Member States are required, under Article 6(1)(e) and Article 12(b), or under subsection (a) of the first subparagraph of Article 14 of Directive 95/46, to provide, for the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151, the right to apply to the authority responsible for keeping the register to erase or block the personal data entered in that register after a certain period of time, or to restrict access to it, it is first necessary to ascertain the purpose of that registration.

In that regard, it is apparent from the recitals and from the title of Directive 68/151 that the purpose of the disclosure provided for by that directive is to protect in particular the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets. To that end, the basic documents of the company concerned should be disclosed in order that third parties may be able to ascertain their contents and other information concerning the company, especially particulars of the persons who are authorised to bind the company.

The Court has already noted, moreover, that the purpose of Directive 68/151 is to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market and that, with that in mind, it is important that any person wishing to establish and develop trading relations with companies situated in other Member States should be able easily to obtain essential information relating to the constitution of trading companies and to the powers of persons authorised to represent them, which requires that all the relevant information should be expressly stated in the register (see, to that effect, judgment of 12 November 1974, Haaga, 32/74, EU:C:1974:116, paragraph 6).

Moreover, it is apparent from the case-law of the Court that the disclosure provided for in Article 3 of Directive 68/151 is intended to enable any interested third parties to inform themselves of these matters, without having to establish a right or an interest requiring to be protected. The Court noted, in that regard, that the very wording of Article 54(3)(g) of the EEC Treaty, on which that directive was based, refers to the need to protect the interests of third parties generally, without distinguishing or excluding any categories falling within the ambit of that term, and consequently the third parties referred to in that article cannot be limited in particular merely to creditors of the company concerned (see judgment of 4 December 1997, Daihatsu Deutschland, C-97/96, EU:C:1997:581, paragraphs 19, 20 and 22, and the order of 23 September 2004, Springer, C-435/02 and C-103/03, EU:C:2004:552, paragraphs 29 and 33).

Furthermore, as to whether, in order to achieve the aim referred to in Article 3 of Directive 68/151, it is

in principle necessary for the personal data of natural persons referred to in Article 2(1)(d) and (j) of that directive to remain on the register and/or accessible to any third party upon request also after the activity has ceased and the company concerned has been dissolved, it should be pointed out that the directive makes no express provision in that regard.

However, as the Advocate General also pointed out in points 73 and 74 of his Opinion, it is common ground that even after the dissolution of a company, rights and legal relations relating to it continue to exist. Thus, in the event of a dispute, the data referred to in Article 2(1)(d) and (j) of Directive 68/151 may be necessary in order, inter alia, to assess the legality of an act carried out on behalf of that company during the period of its activity or so that third parties can bring an action against the members of the organs or against the liquidators of that company.

Moreover, depending in particular on the limitation periods applicable in the various Member States, questions requiring such data may arise for many years after a company has ceased to exist.

In view of the range of possible scenarios, which may involve actors in several Member States, and the considerable heterogeneity in the limitation periods provided for by the various national laws in the various areas of law, highlighted by the Commission, it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary.

In those circumstances, Member States cannot, pursuant to Article 6(1)(e) and Article 12(b) of Directive 95/46, guarantee that the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151 have the right to obtain, as a matter of principle, after a certain period of time from the dissolution of the company concerned, the erasure of personal data concerning them, which have been entered in the register pursuant to the latter provision, or the blocking of that data from the public.

That interpretation of Article 6(1)(e) and Article 12(b) of Directive 95/46 does not, moreover, result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter.

First, Article 2(1)(d) and (j) and Article 3 of Directive 68/151 require disclosure only for a limited number of personal data items, namely those relating to the identity and the respective functions of persons having the power to bind the company concerned to third parties and to represent it or take part in the administration, supervision or control of that company, or having been appointed as liquidator of that company.

Secondly, as pointed out in paragraph 49 of the present judgment, Directive 68/151 provides for disclosure of the data referred to in Article 2(1)(d) and (j) thereof, due, in particular, to the fact that the only safeguards that joint-stock companies and limited liability companies offer to third parties are their assets, which constitutes an increased economic risk for the latter. In view of this, it appears justified that natural persons who choose to participate in trade through such a company are required to disclose the data relating to their identity and functions within that company, especially since they are aware of that requirement when they decide to engage in such activity.

Finally, as regards subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, it must be pointed out that, whereas it follows from the foregoing that, in the weighting to be carried out under that provision, in principle, the need to protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market take precedence, it cannot be excluded, however, that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in their consultation.

In that regard, however, it should be pointed out that, in so far as the application of subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 is subject to the proviso that national law does not lay down a provision to the contrary, the final decision as to whether the natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151 may apply to the authority responsible for keeping the register

for such limitation of access to personal data concerning them, on the basis of a case-by-case assessment, is a matter for the national legislatures.

It is for the referring court to determine the provisions of its national law in that regard.

Assuming that such an examination reveals that national law permits such applications, it will be for the national court to assess, having regard to all the relevant circumstances and taking into account the time elapsed since the dissolution of the company concerned, the possible existence of legitimate and overriding reasons which, as the case may be, exceptionally justify limiting third parties' access to the data concerning Mr Manni in the company register, from which it is apparent that he was the sole administrator and liquidator of Immobiliare Salentina. In that regard, it should be pointed out that the mere fact that, allegedly, the properties of a tourist complex built by Italiana Costruzioni, of which Mr Manni is currently the sole director, do not sell because of the fact that potential purchasers of those properties have access to that data in the company register, cannot be regarded as constituting such a reason, in particular in view of the legitimate interest of those purchasers in having that information."

On those grounds, the Court (Second Chamber) ruled:

"Article 6(1)(e), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, read in conjunction with Article 3 of the First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community, as amended by Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003, must be interpreted as meaning that, as EU law currently stands, it is for the Member States to determine whether the natural persons referred to in Article 2(1)(d) and (j) of that directive may apply to the authority responsible for keeping, respectively, the central register, commercial register or companies register to determine, on the basis of a case-by-case assessment, if it is exceptionally justified, on compelling legitimate grounds relating to their particular situation, to limit, on the expiry of a sufficiently long period after the dissolution of the company concerned, access to personal data relating to them, entered in that register, to third parties who can demonstrate a specific interest in consulting that data."

BIBLIOGRAPHY

Baugh A. C. & Cable T. (2002, 5th ed.). *A History of the English Language.* Oxon, UK: Routledge. Taylor And Francis Group.

Haigh, R. (2015, 4th ed.). *Legal English.* London, New York: Routledge, Taylor and Francis Group.

Jespersen, Otto. Growth and Structure of the English Language. Doubleday Anchor reprint. 9th ed. (1938). Garden City: Doubleday & Company, Inc., 1955.

Maley, Y. (1994). ‚The Language of the Law' in *Language and the Law.* (edited by John Gibbons). London, New York: Longman Group UK Limited.

Melinkoff, D.(1963; 5th printing 1983). *The Language of the Law.* Boston, MA: Little Brown.

Tiersma, P. (1999). *Legal Language.* Chicago: University of Chicago Press.

Walbaum Robinson, Isabel Alice. *The „Word Factory", A Study of the Processes Engaged in the Formation of Legal Terms, Opinio Juris in Comparatione,* Op. J., Vol. 1/2011, Paper n.3.