FRICoRe

Judicial Training Project

Fundamental Rights In Courts and Regulation

CASEBOOK

EFFECTIVE DATA PROTECTION AND FUNDAMENTAL RIGHTS

COUR DE JUSTIC

DE L'UNION

SSM

Scuola Superiore della Magistratura

UNIVERSITY OF TRENTO

THIS PUBLICATION IS FUNDED BY THE EUROPEAN UNION'S JUSTICE PROGRAMME (2014-2020)

Effective Data Protection and Fundamental Rights

Edited by Paola Iamiceli, Fabrizio Cafaggi, Chiara Angiolini

Publisher: Scuola Superiore della Magistratura, Rome – 2022

ISBN 9791280600271

Published in the framework of the project:

Fundamental Rights In Courts and Regulation (FRICoRe)

Coordinating Partner:

University of Trento (*Italy*)

Partners:

Scuola Superiore della Magistratura (*Italy*)

Institute of Law Studies of the Polish Academy of Sciences (INP-PAN) (*Poland*)

University of Versailles Saint Quentin-en-Yvelines (*France*)

University of Groningen (*The Netherlands*)

Pompeu Fabra University (*Spain*)

University of Coimbra (*Portugal*)

Fondazione Bruno Kessler (*Italy*)

The present Casebook builds upon the ReJus Casebook - Effective Justice in Data Protection. In particular, new streams of questions have been added (specifically in chapters 1, 3, 4, 5, 7, 9). Furthermore, new developments have been considered both in EU and national caselaw.

Edition: May 2022

Scientific Coordinator of the FRICoRe Project:

Paola Iamiceli

Coordinator of the team of legal experts on Effective Data Protection:

Paola Iamiceli

Project Manager:

Chiara Patera

Co-editors and Co-authors of this Casebook:

Co-editors: Paola Iamiceli (Project Coordinator), Fabrizio Cafaggi, Chiara Angiolini

Introduction: Fabrizio Cafaggi and Paola Iamiceli

Ch. 1: Sandrine Clavel, Fabienne Jault-Seseke

Ch. 2: Sandrine Clavel, Chiara Angiolini

Ch. 3: Sandrine Clavel, Mateusz Grochowski

Ch. 4: Chiara Angiolini

Ch. 5: Sandrine Clavel, Mateusz Grochowski

Ch. 6: Chiara Angiolini, Sandrine Clavel, Federica Casarosa, Maria Magierska

Ch. 7: Chiara Angiolini, Sandrine Clavel, Fabienne Jault-Seseke, Paola Iamiceli, Katarzyna Południak-Gierz

Ch. 8: Sandrine Clavel, Mateusz Osiecki

Ch. 9: Chiara Angiolini, Sébastien Fassiaux

Note on national experts and contributors:

The FRICoRe team would like to thank Olga M. Ceran for her support in the initial design of the addressed questions and the chapters' editing, and all the judges, experts, and collaborators who contributed to the project and to this Casebook by suggesting national and European case law *(in alphabetical order)*

Chiara Tea Antoniazzi *
Marc Bosmans
Roberta Brusco*
Luigi Cannada Bartoli*
Francesca Capotorti*
Stefano Caramellino*
David Castillejos Simon*
Mélanie Clément-Fontaine*
Aurelia Colombi Ciacchi
Jarosław Czarnota*
Krystyna Dąbrowska
Fiorella Dal Monte*
Silvia Dalle Nogare*
Nicole Di Mattia*
Carmen Domocos*
Lorette Dubois*
Rossana Ducato
Malte Engeler*
Martina Flamini*
Andrea Maria Garofalo
Florence Gaullier*
Inès Giauffret
Karin Kieffer*
Maud Lagelée-Heymann
Lottie Lane
Sandra Lange
Maria Teresa Leacche*
Tobias Nowak
Isabella Oldani*
Aniel Pahladsingh
Charlotte Pavillon
Simon Peers
Romain Perray*
FrancescoPerrone
Piotr Polak
Lyubka Petrova
Gianmatteo Sabatino*
Pedro Santos Azevedo
Wojciech Sawczuk*
Markus Thoma
Sil van Kordelaar
Lavinia Vizzoni*
Margaux Voelckel*
Anne Witters
Célia Zolynski
The students of Master PIDAN* (UVSQ/Sacla)

*: contributors in the framework of the RE-Jus project

Table of Contents:

6. Effective Data protection between administrative and judicial enforcement

6.1. Introduction

To ensure an effective protection of personal data, the EU relies mainly on national supervisory authorities as mentioned in Chapter VI and VII of the GDPR. The role of judicial enforcement should not, however, be underestimated.

Indeed, at the **national level**, data protection is enforced through both administrative and judicial enforcement mechanisms.

With regard to the first one, Article 58 of the GDPR confers to national supervisory authorities a broad catalogue of corrective, investigative, authorisation and advisory powers. All of the EU supervisory authorities have, amongst others, a competence to impose fines, issue a warning or reprimand to the data processor/controller, order the suspension of the processing of personal data, block and erasure of specific data, or order the controller or the processor to comply with the data subject's requests.

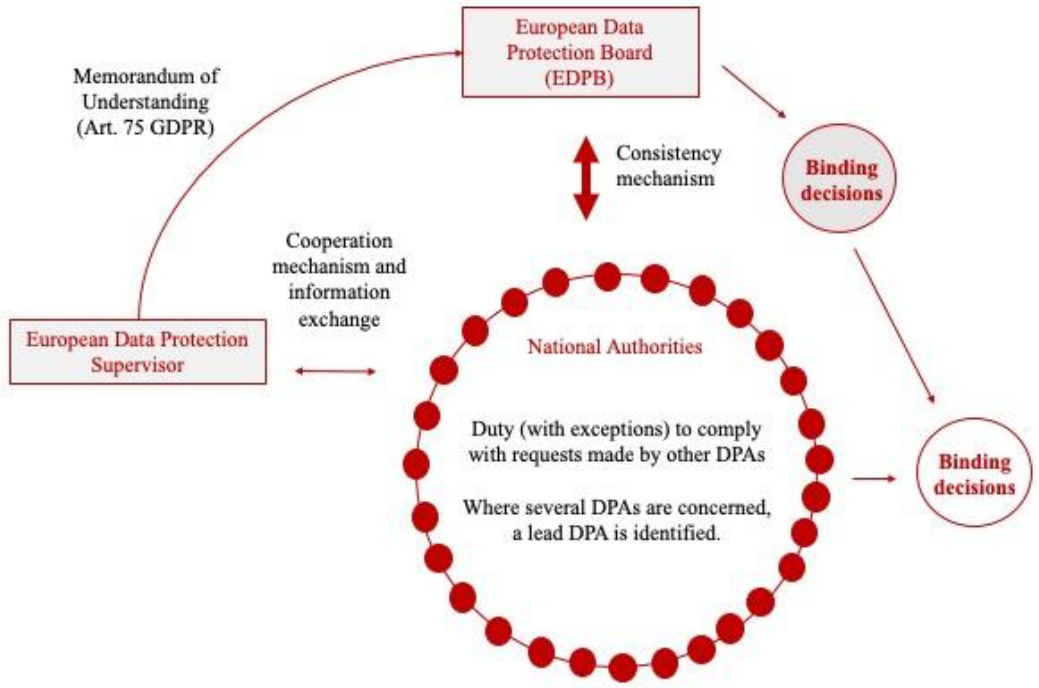
The power to apply financial charges belongs to the supervisory authorities, with the exception of those systems that do not recognise administrative fines (Denmark, Estonia). In the latter case, pursuant to Article 83 (9) of the GDPR, the fine is initiated by the competent supervisory authority and imposed by competent national courts. Recital 151 further specifies that in Denmark the fine is imposed by the national court as a criminal penalty and in Estonia by the supervisory authority in the framework of a misdemeanour procedure. In each case, the competent national courts shall recognise the recommendation of the DPA. A result should be equivalent to the administrative fines issued in other Member States.

At the **European level**, the action of the European Data Protection Supervisor (EDPS) and of the European Data Protection Board (EDPB) are of particular interest. The **European Data Protection Supervisor (EDPS)** is responsible for ensuring the protection of the fundamental rights and freedoms of natural persons and the right to data protection in relation to the processing of personal data by EU institutions and bodies (Article 52, EU Regulation 2018/1725). The tasks of the EDPS mainly relate to the application of EU Regulation 2018/1725 governing the processing of data by EU bodies and organs: this authority deals with complaints, conducts appropriate investigations, provides consultation to EU institutions on the processing of personal data, participates in the European Data Protection Board.

The **European Data Protection Board** (Article 68 GDPR) since 25 May 2018, replaced the Article 29 Working Party (Article 29 Directive 1995/46/EC), and endorsed certain WP29 documents of the Article 29 Working Group with the Endorsement 1/2018, dated May 25, 2018. The Board performs the function of ensuring the consistent application of EU Regulation 2016/679 and has the tasks of monitoring, advising the Commission, publishing guidelines, recommendations and best practices, and issuing opinions on codes of conduct drawn up at the European level (70 EU Regulation 2016/679). Under Article 65, GDPR, in order to ensure the correct and consistent application of the GDPR in individual cases, the Board shall adopt a binding decision where a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. With respect to the activity of the EDPB, although the GDPR does not refer to the principle of good administration, the reference to Article 41 CFREU appears in the Rules of Procedure of the European Data Protection Board, as last modified in October 2020. Article 11 of that rules states:

"The Board shall respect the right to good administration as set out by Article 41 of the Charter. Before taking decisions, the Board shall make sure that all persons that might be adversely affected have been heard".

The complexity of the administrative enforcement required the creation of a system of **coordination between administrative authorities**, which is summarised in the following table:



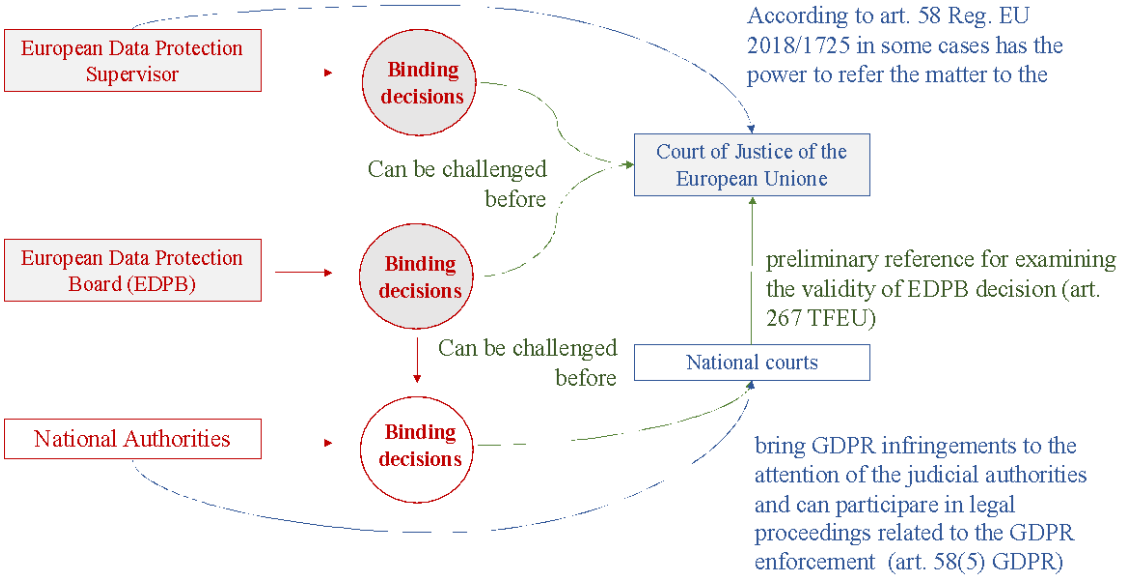
The GDPR provides a "diffuse" mechanism of cooperation between the various authorities and a "centralised" one.

With regard to the former, there is provision for the exchange of information between national supervisory authorities, mutual assistance, within a framework of cooperation. The distribution of competence among national authorities is established on the basis of various criteria, including the establishment of the controller and the existence of a complaint, in order to define both the "concerned" authorities and, in the case of several authorities involved, a lead authority. The coordination and cooperation between the lead authority and the other authorities concerned are regulated in Article 60 of EU Regulation 2016/679, according to which they must work to reach consensus. Within this framework, the supervisory authorities are obliged to comply with requests from other authorities, except for some limited cases. It also provides for the possibility of joint operations.

The 'centralised' cooperation mechanism mainly concerns the relationships between national DPAs and the EDPB, the contribution of national authorities to the activities of the EDPB and a consistency mechanism aimed at ensuring the cooperation of authorities and the uniform application of EU law.

Moreover, with regard to the relationships between the EDPB and the EDPS, Article 69 EU Regulation 2016/679 guarantees its independence in the exercise of the tasks referred to in Article 70 EU Regulation 2016/679, also with respect to the European Supervisor. Furthermore, the relationship between the EDPS and the EDPB is governed, according to Article 75 GDPR, by a memorandum of understanding, adopted on 25 May 2018 by the two Authorities. This document affirms the principles of independence and impartiality of the two authorities, those of good administration, integrity and the principle of cooperation, with a commitment to use the consensus method. In addition, without prejudice to professional secrecy, the two authorities exchange information on a regular basis for the purpose of the effectiveness of the arrangement.

Furthermore, **the relationships between administrative authorities and Courts are of particular interest,** and they are summarised in the following table:



With regard to the dialogue between the supervisory authorities and courts, judicial review is possible at national level against the decisions of the supervisory authority, and in some cases administrative authorities, as well as, at the conditions established by Article 80 GDPR, collective entities, may seek actions before courts.

As to the judicial review of administrative decisions, Article 78 gives an individual the right to an effective judicial remedy against a supervisory authority, and according to Article 58(4) of the GDPR the exercise by the supervisory authority of its powers shall be subject to appropriate procedural safeguards in accordance with Union, Member State law and the Charter, including effective judicial remedy and due process. The GDPR, however, does not clearly identify the extent of the judicial review by courts, i.e., whether it should be limited to the formal correctness of the decision of the supervisory authority (quashing the decision if appropriate, or requiring a new proceeding before the supervisory authority) or whether it may review the form and content of the decision (revising the content of the decision, and the remedies provided by the supervisory authority). Recital 143 explains only that the court "should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute". No decision of the CJEU has addressed this issue in the area of data protection, although in other areas the effectiveness of judicial review has been addressed by the CJEU. For instance, in the *East Sussex Council* case (C-71/14) the CJEU affirmed that, where the European legislation does not detail the scope of judicial review, it is for the legal systems of the Member State to determine that scope, subject to the principles of equivalence and effectiveness[30]. Following the reasoning of the Court in *Puškár*, it seems that the Member States dispose of procedural autonomy as long as it is effective and not disproportionate.

[30] See paragraph 53.

See also the *Berlioz* case in the tax law area, paragraph 89 : "Those provisions of Directive 2011/16 and Article 47 of the Charter must be interpreted as meaning that, in the context of an action brought by a relevant person against a penalty imposed on that person by the requested authority for non-compliance with an information order issued by that authority in response to a request for information sent by the requesting authority pursuant to Directive 2011/16, the national court not only has jurisdiction to vary the penalty imposed but also has jurisdiction to review the legality of that information order. As regards the condition of legality of that information order, which relates to the foreseeable relevance of the requested information, the courts' review is limited to verification that the requested information manifestly has no such relevance."

With respect to the coordination mechanisms between the EDPB and courts, the dialogue can take place at two levels. As far as the European level is concerned, the EDPB's decisions can be challenged before the CJEU by any physical or legal person or by the supervisory authorities (Article 263 TFEU). Moreover, if a decision of the supervisory authority implementing a EDPB decision is challenged before a national court and the validity of the EDPB's decision is in question, that national court has no power to invalidate the EDPB decision, but if it considers the decision invalid must refer the question of validity to the CJEU (Article 267 TFEU as interpreted by the Court of Justice; recital 143 Regulation UE 2016/679).

Main questions addressed:

1. (a) In data protection cases, what is the role of the right to an effective judicial remedy (Article 47 CFREU), in defining the relationship between administrative and judicial enforcement?

(b) How does the right to effective judicial remedy affect coordination of administrative and judicial enforcement?

2. Is there a different institutional design between the administrative and judicial enforcement proposed by the ECtHR jurisprudence and that of the CJEU? When a mandatory preliminary administrative procedure is required before going to court, is it subject to different conditions under CJEU and the ECtHR standards in order to guarantee compliance with the principles of access to justice and the right to a fair trial?

3. a) Does Article 47 CFREU impact coordination between EU institutions and national authorities?

b) Is the supervisory authority of a Member State able to examine the claim of a person regarding the processing of personal data relating to him, and involving the transfer of personal data from a Member State to a third country, where the Commission has previously found that this third country ensures an adequate level of protection?

c) Does Article 47 CFREU impact coordination between national authorities?

4. Is the supervisory authority of a Member State able to examine the claim of a person concerning the validity of an act of the EU?

Cluster of relevant CJEU cases

➢ Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18 **("Facebook Ireland and Schrems/Schrems II")**

➢ Judgment of the Court (Grand Chamber), 15 June 2021, Case C-645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit,* **("Facebook Ireland and Others")**

➢ Judgment of the Court (Second Chamber) of 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, Case C-40/17 **("Fashion ID")**

➢ Judgment of the Court (Second Chamber) of 27 September 2017, Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy, Case C-73/16, ("**Puškár**")

➢ Judgment of the Court (Second Chamber), 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16 ("**Rīgas satiksme"**)

➢ Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ("**Schrems**")

➢ Judgment of the Court (Grand Chamber) of 6 October 2020. *État luxembourgeois v B and Others*, Case C-245/19 and C-246/19

➢ Request for a preliminary ruling from the Fővárosi Törvényszék (Hungary) lodged on 3 March 2021 — *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-132/21 (**BE v Nemzeti**)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 14 December 2021 — *TR v Land Hessen* (Case C-768/21)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 2 February 2022 — *AB v Land Hesse* (Case C-64/22)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 11 January 2022 — UF v Land Hesse (Case C-26/22)

Within this cluster, the aforementioned cases shall be presented as reference points for judicial dialogue within the CJEU and between EU and national courts on the question of the coordination between enforcement systems and the cooperation between national courts and national supervisory authorities.

6.1.1. Question 1: The right to effective judicial remedy and the coordination of administrative and judicial enforcement

(a) In data protection cases, what is the role of the right to an effective judicial remedy (Article 47 CFREU), in defining the relationship between administrative and judicial enforcement?
(b) How does the right to effective judicial remedy affect coordination of administrative and judicial enforcement?

The possible relationships between administrative and judicial enforcement are the following:

a) *Alternative:* National legislation indicates that the national supervisory authority and the courts are alternative means of enforcement with respect to a violation of data protection legislation. The claimant can bring the claim either before an administrative authority or before a court.

b) *Complementary:* National legislation indicates that the national supervisory authority and courts are complementary with respect to a violation of data protection legislation. It defines the relationship between the two bodies. The claimant can bring the same claim before both, and the legislation can impose a sequence, *e.g.,* first the administrative authority and then the court.

a. simultaneous

b. sequential

c) *Independent:* National legislation does not say anything about the relationship between the national supervisory authority and the courts.

Relevant legal sources

EU Level

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Article 22
See, for comparison, Articles77-79, 83(7-8), GDPR
National Level
Slovak Constitution
Article 46

Code of Civil Procedure (Slovak): *Article 20, Paragraph 250v(1) and (3)*

The case(s):

Mr P, a Slovak citizen, presented before the Supreme Court of the Slovak Republic a claim to order the Finance Directorate, all tax offices under its control and the Financial Administration Criminal Office to remove his name from a list of people in directorship positions within companies, previously drawn up by the Finance Directorate. Although the list could only circulate among administrative offices, Mr. P. maintained that such a list, containing the Identity Number and Tax Identification Number of each mentioned individual, constituted a violation of his rights. He asked for the removal of his name and of any reference to him from the list and from other similar lists, as well as from the finance authority's IT system. Mr. P. never claimed nor proved that he had obtained the list with the consent (as was legally required) of the Finance Directorate or the Financial Administration Criminal Office. The Supreme Court dismissed the claim since Mr. P. (as well as the other two applicants) had not exhausted the remedies before the national administrative authorities. Mr. P. then lodged an appeal with the Constitutional Court of the Slovak Republic.
The Slovak Constitutional Court focused mainly on the jurisprudence of Article 6(1) ECHR in connection with Article 46 of the Slovak Constitution. In particular, the Constitutional Court addressed the obligation of the courts to justify their decision taking all the relevant facts and legal elements into account. This obligation was deemed as a prerequisite for the parties to exercise their right to an effective remedy. In this way, the Constitutional Court interprets Article 46 (1) of the Slovak Constitution in accordance with **Article 6 (1) ECHR** and on the basis of the ECtHR jurisprudence (in particular, *Garcia Ruiz v. Spain*; *Van de Hurk v. the Netherlands*; *Ruiz Torija v. Spain*; *Georgiadis v. Greece*; *Suominen v. Finland*; *Vetrenko v. Moldova*; *Wagner and J.M.W.L. v. Luxembourg*; *Pronina v. Ukraine*; *Krasulya v. Russia*; *Hiro Balani v. Spain*).
The Constitutional Court affirmed that in order to comply with the requirements of Article 46 of the Constitution (and Article 6 ECHR) the analysis of the Supreme Court should have taken into account all circumstances of the case in terms of the level of protection of personal data guaranteed by the Constitution and the level of protection of privacy guaranteed by the ECHR. Thus, the Constitutional Court concluded, after having analysed and compared the national and ECtHR jurisprudence, that the Supreme Court had failed to take into account the factual and legal arguments of the case and, most importantly, to provide a decision on the conditions that should have been met for the protection of personal data in the case of data processing by tax authorities.
Thus, the decision of the Constitutional Court completely disregarded the sequence proposed by the Supreme Court ruling between the preliminary administrative proceedings and the judicial proceedings, requiring the court to provide a detailed analysis of the claim and a decision on whether the processing of data by the tax authorities was lawful.
The Constitutional Court then affirmed that the Supreme Court had infringed the applicant's fundamental rights, namely the right to an effective remedy and a fair trial, the right to privacy and the right to protection of personal data. Thus, the Constitutional Court referred the case back to the Supreme Court. At this point, the Supreme Court, believing that the Constitutional Court had not taken into account the case-law of the EU Court of Justice, decided to refer to that court for a preliminary ruling.

Preliminary questions referred to the Court:

The Slovak Supreme Court presented four questions; for the purpose of this analysis, only the first question will be addressed in detail in this section.

The first question sought to verify if the mandatory preliminary administrative procedure adopted by the Slovak legislature in the case at issue is compliant with EU law and in particular with Article 47 CFREU.

"1. Does Article 47(1) of the Charter, under which every person whose rights — including the right to privacy with respect to the processing of personal data in Article 1(1) et seq. of Directive 95/46 — are violated has the right to an effective remedy before a court in compliance with the conditions in Article 47 of the Charter, against a provision of national law which makes the exercise of an effective remedy before a court, meaning an administrative court, conditional on the fact that the claimant, to protect his rights and freedoms, must have previously exhausted the procedures available under *lex specialis* — law on a specific subject — such as the Slovak Law on administrative complaints?"

Reasoning of the Court:

After stating that personal data collected for tax purposes fall within the scope of Directive no. 95/46, since they are dealt with by Article 13 (1) of that Directive, the Court proceeds to consider each of the preliminary questions.

Where the first one is concerned, the Court points out that the obligation to exhaust additional administrative remedies, while not excluded by Directive no. 95/46, must be scrutinised in light of Article 47 CFREU, Article 4 (3) of the TEU (principle of sincere cooperation) and Article 19 (1) of the TEU (effective judicial protection in the fields covered by EU law). Since such an obligation to exhaust additional administrative remedies constitutes a limitation of the right to an effective judicial remedy, it may be justified according to the criteria set in accordance to Article 52 (1) CFREU, namely only when:

i) provided by law;
ii) respectful of the essence of the right;
iii) subject to the principle of proportionality;
iv) compliant with objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

The Court focused in particular on the last two criteria.

With regard to the existence of objectives of general interest, the Court acknowledged that the obligation to lodge an administrative complaint before bringing a legal action has two main positive effects: first, it may relieve the courts of disputes that can be decided in a shorter time by the administrative authority concerned; and second, it may increase the efficiency of judicial proceedings in disputes in which a legal action is brought despite the fact that a complaint has already been lodged. Thus, the general obligation pursued objectives of general interest.

Regarding the test of proportionality, the Court relied on the AG opinion and on the decisions in *Alassini* and *Menini*. In particular, it explicitly referred to the criteria identified in the *Alassini* decision (paragraph 67), which should guide the proportionality test *vis-à-vis* the additional steps imposed in the national procedure, namely:

1. The procedures do not result in a decision which is binding on the parties;
2. The procedures do not cause a substantial delay for the purposes of bringing legal proceedings;
3. The procedures suspend the period for the time-barring of claim;
4. The procedures do not give rise to costs — or give rise to very low costs — for the parties;
5. The procedure must not be accessible exclusively by electronic means, nor be the only means by

which the settlement procedure may be accessed; and,

6. The procedures allow for interim measures in exceptional cases where the urgency of the situation so requires.

On the basis of these criteria, the Court affirmed that the obligation to exhaust the available administrative remedies appears appropriate for achieving the aforementioned objectives of general interest, and no less onerous and efficient method is available and capable of achieving those objectives.

Conclusion of the Court:

The Court declared that the Slovak legal provisions do not as such infringe EU law, and referred to the national court the assessment of the proportionality of the obligation to exhaust administrative remedies, also with regard to the additional costs of the proceedings imposed on the parties.

Elements of judicial dialogue:

The CJEU decision in *Puškár* arises from a preliminary reference under Article 267 TFEU. The Slovak Supreme Court resorted to a preliminary reference owing to a conflict of interpretation with the Slovak Constitutional Court. The CJEU acknowledges that the contrast between the national courts may affect the results of the decision in a specific case; thus, it addresses in detail the problem of coordination between administrative and judicial enforcement systems.
It is important to note that the conclusion of the CJEU is based on the jurisprudence of the same court in other areas of law, namely public procurement (e.g., *SC Star Storage*), migration and asylum law (e.g., decisions in *Tall* and *Sacko*), and in particular electronic communication (e.g., *Alassini*) and consumer protection (e.g. *Menini*).
From a different standpoint, the judicial dialogue between European and national courts at the same time addresses the horizontal aspect, with the decision of the CJEU able to provide a uniform interpretative perspective so to avoid further conflicts.
In Rīgas satiksme a question concerning the relationship between administrative and judicial enforcement has been raised and concerned the disclosure of personal data of a person responsible for a road accident to a third party in order to exercise a legal claim. However, the CJEU in this case did not address the manner in which the two enforcement mechanisms interact. It rather focused on the balance of interests between the protection of personal data and the possibility to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data (see more in Chapter 3, question 2).
In *Fashion ID* the Court, while not referring directly to the problem of coordination between administrative and judicial enforcement systems, evokes *Puškár* in the interpretation of Article 22 of the Directive. The Court followed the reasoning of *Puškár* where it confirmed that although Article 22 requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law, it does not contain any provisions specifically governing the conditions under which that remedy may be exercised.

In the pending case *BE v Nemzeti* (C-132/21) the referring Court asked to the CJEU the following questions concerning the relationship between administrative and judicial enforcement:

"In the event that the data subject (…) simultaneously exercises his right to lodge a complaint under Article 77(1) [GDPR] and his right to bring a legal action under Article 79(1) [GDPR], may an interpretation in accordance with Article 47 of the Charter of Fundamental Rights be regarded as meaning:

(a) that the supervisory authority and the court have an obligation to examine the existence of an infringement independently and may therefore even arrive at different outcomes; or

(b) that the supervisory authority's decision takes priority when it comes to the assessment as to whether an infringement has been committed, regard being had to the powers provided for in Article 51(1) of Regulation 2016/679 and those conferred by Article 58(2)(b) and (d) of that regulation?

3. Must the independence of the supervisory authority, ensured by Articles 51(1) and 52(1) of Regulation 2016/679, be interpreted as meaning that that authority, when conducting and adjudicating upon complaint proceedings under Article 77, is independent of whatever ruling may be given by final judgment by the court having jurisdiction under Article 79, with the result that it may even adopt a different decision in respect of the same alleged infringement?"

Lastly, in the pending case *AB v Land Hesse* (Case C-64/22), the referring court asked to the CJEU whether according to Article 77(1) GDPR, read in conjunction with Article 78(1) thereof, the outcome that the supervisory authority reaches and notifies to the data subject

(a) has the character of a decision on a petition. The national judge specify that this would mean that judicial review of a decision on a complaint taken by a supervisory authority in accordance with Article 78(1) GDPR is, in principle, limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, or

(b) is to be understood as a decision on the merits taken by a public authority. The national judge specify that this would mean that a decision on a complaint taken by a supervisory authority would be subject to a full substantive review by the court in accordance with Article 78(1) of the GDPR, whereby, in individual cases — for example where discretion is reduced to zero — the supervisory authority may also be obliged by the court to take a specific measure within the meaning of Article 58 of the GDPR.

In the pending case *UF v Land Hesse* (Case C-26/22) the national judge raised similar questions.

Impact on national case law in Member States other than the state of the court referring the preliminary question to the CJEU:

ITALY

Although not directly applying the decision taken in *Puškár*, before the entry into force of the GDPR the Italian Supreme Court addressed the compatibility with Article 24 of the Italian Constitution of the alternative enforcement proceedings before the supervisory authority and before the judicial courts (excluding in the case of a claim before the civil courts the possibility for a data subject to present the same claim before the supervisory authority, and vice versa).[31] In decision no. 6775/2016, 7 April 2016, the Supreme Court (Labour law section) concluded that Article 145 of the Italian Data Protection Code (now repealed) providing for the two alternative enforcement mechanisms is compatible with Article 24 of the Constitution (and therefore compatible with the right of the data subject to a defence) in cases where the claim addresses the "same object". In this sense, the alternative proceedings follow the general procedural rules of *lis pendens*. Whereas, when the claim before the judicial authority addresses the compliance of the data processor with a decision of the supervisory authority and/or the action for pecuniary or moral damages, the choice between the two alternative enforcements cannot apply (similarly, also, in Supreme Court no. 19534/2014, 17 September 2014).

[31] Note that Article 24 of the Italian Constitution provides that:
"Anyone may bring cases before a court of law in order to protect their rights under civil and administrative law. Defence is an inviolable right at every stage and instance of legal proceedings.
The poor are entitled by law to proper means for action or defence in all courts.
The law shall define the conditions and forms of reparation in case of judicial errors." (official translation)

AUSTRIA

The question of whether a citizen may file a complaint not only before the supervisory authority but also before the national court appeared in the Maximillian Schrems lawsuit against Facebook Ireland Ltd, filed before the Austrian court in 2014. During the proceedings, Facebook argued that only the Irish DPA should be responsible for the case. The Vienna Regional Court found itself twice not competent to consider the lawsuit — the second time in December 2018, after the Court's decision in case C-498/16 (*Schrems II*).

In the decision 11 R 24/19h, 25 March 2019, the Higher Regional Court of Vienna ("Oberlandesgericht Wien") admitted the right to submit the civil lawsuit before the national court on the grounds of Article 79 of the GDPR. The Court derived from this provision that Article 17 (1a) of the GDPR and §45 (2) of the Austrian Data Protection Act (DSG) asserted the right to erasure also in the judicial proceedings. According to the Court, §29 (1) DSG that standardises the jurisdiction for claims for damages does not stand in the way because it is only *lex specialis* to the GDPR.

POLAND

In Poland, there has not been any case directly approaching the issue discussed in *Puškár* so far. However, the question of coordination between judicial and administrative enforcement may appear in the recently opened case before the District Court in Warsaw.

Wojciech Klicki, a lawyer and privacy activist, sued the Polish Post for violating the GDPR by processing data of Polish citizens without a clear legal basis. The case concerns preparations for presidential elections which due to the COVID-19 pandemic were supposed to take place via mail on the 10 of May 2020 (eventually they were postponed). However, the law introducing the new form of elections came into effect on the 9 of May 2020. Nevertheless, the Polish Post had demanded from municipalities access to electoral register already on 16 of April 2020. After their refusal, it turned out that the Post had already had access to the social security number register from the Ministry of Digitalisation They argued that the decision of the Prime Minister was a legitimate basis for the processing.

The Polish data protection authority agreed with that interpretation and claimed that there had been no violation of the GDPR. The DPA did not initiate any proceedings but issued a statement where he argued that the PM's decision constituted a legitimate basis for the processing. Hence, the lawyer decided to pursue a judicial recourse instead of an administrative one.

According to Polish law, the court has to inform the DPA about the proceeding. The court should also suspend the process if the DPA initiated its own examination. So far the authority refused to take any action, arguing that the processing is legal. However, it may join the judicial proceedings before the District Court. While assessing compensation for the damage caused by infringement of data protection laws, the court is bound by the DPA's decision assessing the scope of those infringements.

6.1.2. Question 2: Interaction between the CJEU and the ECtHR

Is there a different institutional design between the administrative and judicial enforcement proposed by the ECtHR jurisprudence and that of the CJEU? When a mandatory preliminary administrative procedure is required before going to court, is it subject to different conditions under CJEU and the ECtHR standards in order to guarantee compliance with the principles of access to justice and the right to a fair trial?

Relevant legal sources:

ECHR Level

Article 6(1) ECHR

"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

The analysis:

The issue of the distinction between the approaches of ECtHR and CJEU jurisprudence was mentioned in the *Puškár* case described above. In particular, the Slovak Supreme Court presented a fourth question seeking to resolve the conflict of jurisprudence between the CJEU and the ECtHR emerging from the interpretation by the Constitutional Court of the interconnection between the right to an effective legal remedy and the right to data protection. However, the Slovak Supreme Court in its preliminary reference did not clarify which were the specific decisions leading to the alleged conflict. This affected the ability of the CJEU to reply.

Although the CJEU did not provide a response regarding the potential "conflict" between its case-law and that of the ECHR, since this was raised in too general terms, for the purpose of the present analysis, it is useful to examine whether the European courts adopt different approaches with regard to the exercise of the right to an effective legal remedy in case of mandatory administrative proceedings in order to comply with Articles 47 CFREU and 6 ECHR, respectively.

The relevant ECtHR jurisprudence on the right to a fair trial includes cases addressing the following issues:

a. the inclusion of preliminary administrative procedure, and
b. the reasonable length of the proceedings.

Under a., the ECtHR acknowledged that the right of access to the courts is not absolute. In this sense, the prior intervention of administrative and professional bodies can be justified by the demands of flexibility and efficiency (see ECtHR decision in *Le Compte, Van Leuven and De Meyere v. Belgium*, § 51). In particular, the Strasbourg court found no violation if judicial bodies do not in themselves satisfy the requirements of Article 6 ECHR, insofar as the proceedings before those bodies are "*subject to subsequent control by a judicial body that has full jurisdiction*" and does provide the Article 6 guarantees (see ECtHR decision in *Zumtobel v. Austria*; *Bryan v. the United Kingdom*).[29]

Under b., the ECtHR has developed a broad jurisprudence addressing the importance of administering justice without delays that might jeopardise its effectiveness and credibility. Thus, a positive obligation is imposed on the Member States: to organise their judicial systems in such a way that courts are able to guarantee everyone's right to a final decision on disputes concerning civil rights and obligations within a reasonable time (*Comingersoll S.A. v. Portugal*; *Lupeni Greek Catholic Parish and Others v. Romania*). In order to evaluate the reasonable time in practice, all of the proceedings should be taken into account (*König v. Germany*).

In this sense, it is important to note that the application of Article 6(1) ECHR also takes into account proceedings which, although not wholly judicial in nature, are nonetheless subject to close supervision by a judicial body (see ECtHR decision in *Siegel v. France*). Thus, in order to define the duration of the whole procedure, the non-judicial proceedings are to be taken into account in calculating the reasonable time. Similarly, this happens when an application to an administrative authority is a prerequisite for bringing court proceedings (see ECtHR decisions in *König v. Germany*; *X v. France*; *Kress v. France*). The jurisprudence of the ECtHR does not indicate a precise timeframe for complex procedure, however, it

has affirmed that delays caused by the conduct of non-judicial authorities are deemed as violations of Article 6 (see ECtHR decision in *Schouten and Meldrum v. Netherlands*; *Kritt v. France*; *Clinique Mozart SARL v. France*).
From the analysis above, it emerges that the ECtHR does not differ from the position of the CJEU in regard to the compatibility of a preliminary administrative procedure with the right to a fair trial, insofar as it provides for a subsequent judicial review by a court with full jurisdiction. However, the ECHR has not addressed the case where this procedure is mandatory, whereas the CJEU, as early as the *Alassini* decision, provided a clear set of guidelines to evaluate whether the additional step in the procedure can be deemed compatible with the right to an effective remedy.
With regard to the reasonable length of the proceedings, the ECtHR provides a standard that takes into account whether the inclusion of administrative and non-judicial proceedings may affect the duration of the overall procedure. In this sense, the ECtHR standard is more detailed than the CJEU standard defined in the *Alassini* and *Puškár* decisions and may complement the latter.

6.2. Administrative authorities and effective protection of data subjects

DPA may not refer questions to the CJEU and Article 47 does not directly apply to those. However, the CJEU has had the chance to decide over questions concerning the role of DPAs in ensuring effective protection of data subjects, either as single authorities (question 3) or by means of cooperation among several DPAs (question 4)

6.2.1. Question 3: Coordination between EU institutions and national authorities

a) Does Article 47 CFREU impact coordination between EU institutions and national authorities? b) Is the supervisory authority of a Member State able to examine the claim of a person regarding the processing of personal data relating to them, and involving the transfer of personal data from a Member State to a third country, where the Commission has previously found that this third country ensures an adequate level of protection?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

Relevant legal sources:

Directive 95/46 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
Article 25 (6); Article 28 (3)

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)
Article 46 (2); Article 46 (3) (4); Article 52 (2); Article 52 (4)

The case(s) and preliminary questions referred to the Court:

As presented above in Chapter 1 on territorial scope, *Schrems* (C-362/14) concerned a transfer of the personal data of EU residents to servers belonging to the US, where they were processed.
The High Court of Ireland, hearing the appeal against the decision of the Irish Data Protection Commissioner, decided to present a preliminary reference asking:

"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?"

Reasoning of the Court

Focusing on the interplay between national supervisory bodies, national and European courts regarding the competence to verify the level of protection offered by third countries, the Court distinguishes two scenarios:

1. In the first scenario, pursuant to Article 25(1), the Member State should assess the adequacy of the level of the level of protection of personal data. In this case, on the basis of Article 8 CFREU and Article 28 of Directive 95/46, the Court attributes the responsibility for monitoring compliance with EU rules to the national supervisory authorities.
2. In the second scenario, by contrast, the Member State, the national supervisory authorities (and the courts) are bound by the decision of the Commission affirming that there is compliance with the level of protection. In this case, neither the Member State nor the national supervisory authorities may evaluate or even contest the Commission's evaluation, by adopting decisions or accepting behaviours contrary to the decision.

However, the Court acknowledges that it would be contrary to the system provided by Directive 95/46, and implicitly contrary to the right to an effective remedy, if a national supervisory authority could not examine a claim concerning the protection of a person's rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.

Elements of judicial dialogue

After *Schrems* (C-362/14) it was revealed that Facebook had never relied on the Safe Harbour in transatlantic data transfer but used standard contractual clauses instead. Maximillian Schrems filed a complaint before the Irish Data Protection Commissioner, demanding the DPC to prohibit or suspend the transfer of his personal data to Facebook. The DPC argued that the case concerns the validity of the Decision 2010/87 on standard contractual clauses and initiated a proceeding against Schrems and Facebook.
Then, in the follow up case ***Facebook Ireland and Schrems* (C-311/18),** which concerns a data transfer to the US on the grounds of standard contractual clauses, the High Court of Ireland referred to the Court, amongst others, a following preliminary question:

"If a third country data importer is subject to surveillance laws that in the view of a [supervisory authority] conflict with [the standard contractual clauses] or Article 25 and 26 of Directive [95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of the Directive to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [Decision 2010/87 on standard contractual clauses], or can a [supervisory authority] use its discretion not to suspend data flows?"

The CJEU in its decision applied the GDPR instead of Directive 95/46 because of the entry into force of the former and the lack, in the present case, of a decision taken relying on the Directive.
The CJEU considered that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In that case, the Court stated that it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.
Furthermore, the CJEU, relying on *Schrems* (C-362/14) affirmed that under Article 288(4) TFEU a Commission adequacy decision is, in its entirety, binding to all the Member States to which it is addressed and is therefore binding to all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data. Accordingly, the Court considered that, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, 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 and, as a result, to suspend or prohibit transfers of personal data to that third country.
Nevertheless, the Court stated that:

- a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data.
- a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) CFREU and Article 51(1) and Article 57(1)(a) of the GDPR. Accordingly, the CJEU stated that, even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of their rights and freedoms in regard to the processing of personal data relating to them, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity.

-

6.2.2. Question 3c: The cooperation between national authorities and the right to seek action of national not-leading DPA

Does Article 47 CFREU impact coordination between national authorities?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Grand Chamber), 15 June 2021, Case C-645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit,* **("Facebook Ireland and Others")**

Relevant legal sources:

EU law

Regulation 2016/679

Recitals 1, 4, 10, 11, 13, 22, 123, 141 and 145; Article 3 concerning the territorial scope; Article 4 in relation to the definitions of "main establishment", "cross-border processing"; Article 51 headed 'Supervisory authority'; Article 55 headed 'Competence'; Article 56 headed 'Competence of the lead supervisory authority; Article 57(1) headed 'Tasks"; Article 58(1), (4) and (5) headed 'Powers'; Article 60, headed 'Cooperation between the lead supervisory authority and the other supervisory authorities concerned'; Article 61(1) headed 'Mutual assistance'; Article 62 headed 'Joint operations of supervisory authorities'; Article 63, headed 'Consistency mechanism'; Article 64 (4), headed Opinion of the Board; Article 65(1) headed 'Dispute resolution by the Board'; Article 66(1) and (2) headed 'Urgency procedure'; Article 77 headed 'Right to lodge a complaint with a supervisory authority'; Article 78 headed 'Right to an effective judicial remedy against a supervisory authority'; Article 79 headed 'Right to an effective judicial remedy against a controller or processor',

The case

On 11 September 2015, the President of the Privacy Commission brought legal proceedings seeking an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium before the Dutch-language Court of First Instance, Brussels, Belgium. The object of those injunction proceedings was to bring to an end what the Privacy Commission describes, *inter alia*, as a 'serious and large-scale infringement, by Facebook, of the legislation relating to the protection of privacy' consisting in the collection by that online social network of information on the internet browsing behaviour both of Facebook account holders and of non-users of Facebook services using various technologies. Those features permit Facebook to obtain certain data of an internet user who visits a website page containing features, such as the address of that page, the 'IP address of the visitor to that page, and the date and time of the visit in question. By judgment of 16 February 2018, the Dutch-language Court of First Instance of Brussels held that it had jurisdiction to give a ruling on those injunction proceedings, in so far as the action concerned Facebook Ireland, Facebook Inc., and Facebook Belgium. On the substance, that court held an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium. On 2 March 2018 Facebook Ireland, Facebook Inc., and Facebook Belgium brought an appeal against that judgment before the Brussels Court of Appeal. Before that court, the DPA acts as the legal successor both of the President of the Privacy Commission, who had brought the injunction proceedings, and of the Privacy Commission itself. The referring court held that it has jurisdiction solely to give a ruling on the appeal brought in so far as that appeal concerns Facebook Belgium. Conversely, the referring court held that it lacked jurisdiction to hear that appeal in relation to Facebook Ireland and Facebook Inc. Before giving a ruling on the substance of the main proceedings, a question raised by the referring court is whether the DPA had the required standing and interest to bring proceedings. With regard to the facts subsequent to 25 May 2018, Facebook Belgium claims that the DPA has no competence and has no right to bring such an action given the existence of the 'one-stop shop' mechanism now provided for under the provisions of Regulation 2016/679. On the basis of those provisions, it is claimed that only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings against Facebook Ireland, the latter being the sole controller of the personal data of the users of the social network concerned within the EU.

Preliminary question referred to the Court:

In the view of the referring court, the question that arises is whether, with respect to the facts subsequent to 25 May 2018, the DPA may bring an action against Facebook Belgium, since Facebook Ireland has been identified as the controller of the data concerned. Since that date and by virtue of the 'one-stop shop' rule, it appears that, in accordance with Article 56 of Regulation 2016/679, only the Data Protection Commissioner (Ireland) is competent, subject to review only by the Irish courts. Therefore, the national court referred several questions to the CJEU. The following question focuses on the impact of Article 47 CFR:

'Should Article 55(1), Articles 56 to 58 and Articles 60 to 66 of [Regulation 2016/679], read together with Articles 7, 8 and 47 of the [Charter], be interpreted as meaning that a supervisory authority which, pursuant to national law adopted in implementation of Article 58(5) of that regulation, has the competence to initiate or engage in legal proceedings before a court in its Member State against infringements of that regulation cannot exercise that competence in connection with cross-border data processing if it is not the lead supervisory authority for that cross-border data processing?'

Reasoning of the Court:

Firstly, the Court considered that the exercise of the power of a Member State's supervisory authority to bring actions before the courts of that State cannot be ruled out where, after the mutual assistance of the lead supervisory authority has been sought, under Article 61 of Regulation 2016/679, the latter does not provide the former with the requested information. The CJEU held that in that situation the supervisory authority concerned may adopt a provisional measure in the territory of its own Member State (Article 61(8) GDPR) and, if it considers that there is an urgent need for the adoption of final measures, that authority may request an urgent opinion or an urgent binding decision from the European Data Protection Board (Article 66(2) GDPR). Further, the Court, relying on Article 64(2) GDPR, affirmed that a supervisory authority may request that any matter that is of general application or that produces effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance imposed on it by Article 61 GDPR. Moreover, the Court recalled that, following the adoption of such an opinion or such a decision, and provided that the EDPB approves, after taking account of all the relevant circumstances, the supervisory authority concerned must be able to take the necessary measures to ensure compliance with the rules on the protection of the rights of natural persons as regarding the processing of personal data contained in Regulation 2016/679 and, for that purpose, exercise the power conferred on it by Article 58(5) of that regulation.

As to the compatibility of these rules with Article 47 of the Charter, the Court stated that the manner in which the possibility that a supervisory authority other than the lead supervisory authority may exercise the power laid down in Article 58(5) of Regulation 2016/679, with respect to an instance of cross-border processing of personal data, is circumscribed takes nothing away from the right of every data subject, laid down in Article 78(1) and (2) of that regulation, to an effective legal remedy, in particular, against a legally binding decision of a supervisory authority concerning them, or against a failure by the supervisory authority which has the competence to adopt decisions under Articles 55 and 56 of that regulation, read together with Article 60 thereof, to handle a complaint that that data subject has lodged.

Furthermore, the Court stated that it is clear, in particular, from Article 51(1) of Regulation 2016/679 that the supervisory authorities are responsible for monitoring the application of that regulation, for the purpose, *inter alia*, of protecting the fundamental rights of natural persons regarding the processing of their personal data. Accordingly, the Court stated that the rules on the allocation of competences to adopt decisions between the lead supervisory authority and the other supervisory authorities, as laid down by that regulation, take nothing away from the responsibility incumbent on each of those authorities to

contribute to a high level of protection of those rights, with due regard to those rules and to the requirements of cooperation and mutual assistance. In the same vein, the CJEU considered that the use of the 'one-stop shop' mechanism cannot under any circumstances have the consequence that a national supervisory authority, in particular the lead supervisory authority, does not assume the responsibility incumbent on it under Regulation 2016/679 to contribute to providing effective protection of natural persons from infringements of their fundamental rights as recalled in the preceding paragraph of the present judgment, as otherwise that consequence might encourage the practice of forum shopping, particularly by data controllers, designed to circumvent those fundamental rights and the practical application of the provisions of that regulation that give effect to those rights.

Conclusion of the Court:

The Court concluded that Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation (EU) 2016/679 (GDPR), read together with Articles 7, 8 and 47 CFREU must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to transpose Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross-border data processing even though it is not the 'lead supervisory authority', within the meaning of Article 56(1) of that regulation, with respect to that data processing, provided that that power is exercised in one of the situations where Regulation 2016/679 confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation and that the cooperation and consistency procedures laid down by that regulation are respected.

Elements of judicial dialogue

The CJEU assessed the competences of DPAs under the directive 95/46 in Holstein (C-210/16), and the differences between the rules provided for by the directive and the system introduced with the GDPR seems evident comparing Facebook Ireland and Others (C-645/19) with Holstein (C-210/16). As to the latter, the CJEU affirmed that Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the EU has several establishments in different Member States, the supervisory authority of a Member State was entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the EU, to an establishment situated in another Member State. Furthermore, the CJEU in Holstein (C-210/16) stated that according to Directive 95/46 where the supervisory authority of a Member State intends to exercise its powers of intervention (Article 28 (3) with respect to an entity established in the territory of that Member State, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independent of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.

Lastly, in the pending case TR v Land Hessen (Case C-768/21) the referring court asked as to whether, according to Article 57(1)(a) and (f), Article 58(2)(a) to (j) GDPR, read in combination with Article 77(1) thereof, where the supervisory authority finds that data processing has infringed the data subject's rights, the supervisory authority must always take action in accordance with Article 58(2) of that regulation.

6.2.3. Question 4: Duty of cooperation of national authorities regarding the possible invalidity of an EU act

Is the supervisory authority of a Member State able to examine the claim of a person concerning the validity of an act of the EU?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

Relevant legal sources:

EU Level

Article 28(3) Directive 95/46
Article 58 GDPR

The case and preliminary question referred to the Court:

The problem of the role of the supervisory authority *vis-à-vis* the role of the courts was not addressed directly in the preliminary questions referred in the *Schrems* case (C-362/14) (see description of the case in Chapter 1 on territorial scope). However, in order to identify which authority is responsible for ruling on the validity of a European act, the CJEU addressed, in detail, the duty of cooperation between a supervisory authority and a court.
In a follow-up case *Facebook Ireland and Schrems* which concerns a data transfer to the US on the grounds of standard contractual clauses, the High Court of Ireland referred to the Court, amongst others, a preliminary question whether a data protection authority is required to suspend data flows if a third country data importer is subject to surveillance laws and hence does not comply with the GDPR and the Charter. In the ruling the Court approached the duty to cooperate between national authorities and the courts, as well as general obligation to consider with all due diligence a complaint lodged by an individual on the grounds of Article 77 of the GDPR.

Reasoning of the Court:

In the implementation of an act of the EU, several actors, including national supervisory authorities and courts, may find a lack of compatibility of such act with the fundamental rights and freedoms. However, neither the supervisory authorities nor the courts have the power to declare an EU act invalid. The exclusive jurisdiction to rule on the validity or invalidity of an EU act lies with the CJEU. This is based on legal certainty and the uniform application of EU law.
Additionally, given the specific features of supervisory authorities, the latter do not fall within the definition of "tribunal" in Article 267 TFEU, thus they do not have the possibility of referring questions for preliminary rulings to the CJEU. As a matter of fact, though, the supervisory authorities constitute the first step in the evaluation of the validity of EU acts, and there must be cooperation between the supervisory authorities and the national courts in order to access the CJEU.
Therefore, the different actors may play different roles in the following scenarios:

1) an individual may present a claim before the national supervisory authority, claiming the incompatibility of an EU act with fundamental rights and freedoms. The national supervisory authority concludes that the claim is unfounded. Then, the claimant should, pursuant to Article 28(3) of Directive

95/46[32] read in light of Article 47 CFREU, have access to judicial remedies enabling him to challenge such a decision before the national courts. In this case, if the national courts do not share the evaluation of the supervisory authority and still have doubts regarding the compatibility of the EU act with fundamental right and freedoms, they must present a preliminary question to the CJEU.

2) An individual may present a claim before the national supervisory authority, claiming the incompatibility of an EU act with fundamental rights and freedoms. The national supervisory authority concludes that the claim is founded. Then the supervisory authority, pursuant to Article 28(3) of Directive 95/46[33] must, particularly, in light of Article 8(3) CFREU, be able to institute legal proceedings. In this case, the supervisory authority may put forward its doubts regarding the validity of the EU act, and if the national courts share them they will submit a reference for a preliminary ruling for the purpose of examining the decision's validity.

In *Facebook Ireland and Schrems* (C-311/2018) the Court confirmed that the formula introduced in *Schrems* (C-362/14) may be applied in the environment of the GDPR as well. In the ruling the Court shared the opinion of the Advocate General that the findings in *Schrems* regarding the duty to cooperate between national authorities and the courts may be applied by analogy to EU acts other than an adequacy decision, such as Decision 2010/87 on standard contractual clauses. The supervisory authorities are obliged to consider with all due diligence a complaint lodged by an individual on the grounds of Article 77 (1) of the GDPR.

According to the Court, if a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. Furthermore, the Court confirmed the DPA's obligation to suspend or prohibit a transfer of personal data to a third country if, in its view, the standard data protection clauses cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer. In order to avoid possible divergences among the DPAs, the Court reminded that a supervisory authority may refer the matter to the European Data Protection Board which may adopt a binding decision.

In the case where the Commission has issued and adequacy decision, the Court confirmed that the DPAs cannot individually suspend or prohibit data flows to the third country in question until invalidation of the decision in question. However, the Court stressed that existence of an adequacy decision does not prevent individuals from lodging a complaint before the competent national supervisory authority under Article 77(1) of the GDPR. The DPA is then obliged to consider the complaint and exercise its powers with complete independence.

Subsequently, the Court followed reasoning of *Schrems* and opinion of the AG, confirming that in cases where there may appear doubts around the validity of an EU act, the DPA shall act under requirements of Article 58(5) of the GDPR and Article 8(3) of the Charter and initiate legal proceedings before national courts which further submit a reference for a preliminary ruling. This will concern Commission's adequacy decisions pursuant to Article 45 (3 and 5), decisions on the code of conduct (Article 40 (9) and.

Moreover, the question of a possible invalidity of the act of EU body may appear as well in the context of consistency procedures before the EDPB. Amongst others, the binding decisions issued by the Board

[32] In particular, Article 28(3) (in fine) provides that "Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

[33] In particular, Article 28(3) (last indent) provides that each authority shall be endowed with "the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities."

as a result of a dispute resolution may also be a subject of claims. Recital 143 to the GDPR explains that, following Article 263 TFEU, any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court. The right to challenge them makes the DPAs the sole addressees, and a controller, processor or complainant where the EDPB's decisions concern them directly.

Recital 143 further explains that the national court has no power to declare the Board's decision invalid and must refer the question of validity to the Court in accordance with Article 267 TFEU. A national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU (see also the Introduction of this chapter).