Judicial Training Project

Roadmap To European Effective Justice (Re-Jus): Judicial Training Ensuring Effective Redress To Fundamental Rights Violations

EXECUTIVE SUMMARY

OF THE DATA PROTECTION CASEBOOK

THE RE-JUS PROJECT IS CO-FUNDED BY THE JUSTICE PROGRAMME OF THE EUROPEAN UNION
(JUST/2015/JTRA/AG/EJTR/8703)

Published in October 2018

Executive Summary

1. **Evolution of data protection law -** Since 1995, the EU legislature has addressed the need to protect citizens' data across Member States with the aim of facilitating internal cross-border data transfers within the EU. The need to harmonise legislation across MS proved more compelling as different standards were applied under the different legislation in force, with different levels of protection potentially hampering the free flow of personal data.

2. Faced with a level of fragmentation and divergence in MS data protection legislation that was no longer tolerable, the EU embarked on a wide-ranging reform in the field of data protection. Among the most compelling, though sensitive, needs to emerge was the updating of Directive 95/46 in order to remove the potential obstacles to the free flow of data and enhance data subjects' protection, and to keep pace with the technological developments that in twenty years had radically changed social and economic conditions in the market. The long negotiation process resulted in the adoption, in 2016, of the General Data Protection Regulation. The choice of a Regulation was designed to achieve harmonisation, as the regulation is directly applicable; however, it contains clauses that allow latitude for national specificities.

3. **The impact of Charter of Fundamental Rights -** Through the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights became binding and the right to the protection of personal data enshrined in article 8 of the Charter acquired recognition and autonomy vis-à-vis the right to respect of private life. This fundamental right required detailed implementation by the enactment of data protection legislation at European and national level, and imposed the definition of remedies. Although the CJEU has explicitly addressed the coordination between articles 8 and 47 of the Charter only on a few occasions, in several other cases the Court has adjudicated on the basis of the principle of effectiveness, steering towards a high standard for data protection.

4. **Judicial dialogue -** This Casebook focuses on the judicial dialogue emerging across European and national courts in the area of data protection. This methodology allows analysis of the full cycle of the case, starting from the preliminary reference, through the preliminary ruling, to the follow up judgment and the impact of the European decision in MS different from the referring state.

5. This analysis provides for a wider picture regarding the interplay between European and national courts, showing whether and how the preliminary reference tool is used by courts strategically, either in the way the question is framed by the national court or in the way the national court interprets and applies the CJEU decision in its follow up.

Impact of the Charter on the territorial scope of data protection

7. Extraterritoriality is the subject of important debates in the field of data protection. Before the GDPR, the level of protection under national legislation implementing the European directives varied across MS, raising questions as to which law was applicable to cross-border processing, the jurisdiction of courts in litigation related to cross-border processing, and the territorial reach of the powers of national supervisory authorities.

8. Question 1 (a) & (b) - In the light of the principle of effectiveness, how should the concept be defined of 'processing of data carried out in the context of the activities of an establishment of the controller or processor' in the Union, which constitute the relevant criteria for defining the territorial scope of EU data protection?

9. The jurisprudence of the CJEU, starting with *Google Spain*, although not expressly referring to article 47 CFR, relies on the principle of effectiveness to underline that given the objective of ensuring an 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, the words "carried out in the context of the activities" of an establishment cannot be interpreted restrictively. The approach is confirmed in *Weltimmo*, where the CJEU states that the concept of 'establishment' should be given a flexible definition, which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, both the degree of stability of the arrangements and the effective exercise of activities in a Member State other than the one where the controller's company is registered, must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.

10. Given the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question. Moreover, in order to attain that objective, it should be considered that the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one and even if it does not consist in actual processing as long as it is "inextricably linked" to the processing — exercised through stable arrangements. However, in the decision in *Amazon*, the CJEU specifies that the establishment cannot exist in a Member State merely because the undertaking's website is accessible there.

11. The GDPR solves this issue by providing, in article 3, that the Regulation applies either to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not", or to "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union", if certain connecting factors are found to exist (article 3 (2)).

12. Question 2 - Should the data protection authority of a Member State exercise competence to hear claims lodged by persons victims of unlawful processing of their personal data, where the law of another Member State is applicable because the data processing was carried out in the context of the activities of an establishment of the controller situated on the territory of that Member State?

13. According to the CJEU in *Weltimmo*, the supervisory authority of a Member State may examine that complaint irrespective of the applicable law, and, consequently, even if the law applicable to the processing of the data concerned is that of another Member State. The CJEU shows concern for the effective access to justice and protection of data subjects: a victim of an unlawful practice should be able to seek protection from the data protection authority of the MS where he is domiciled. It is then up to this authority to exercise its powers within the territory of its own Member State or, if powers are to be exercise beyond these limits, to cooperate with the data protection authority of the Member State where the data controller carries out its activities. This conclusion is reaffirmed and strengthened in *Holstein*.

14. Question 3 - Can a national data protection authority exercise its powers against a data controller, when the data controller carries out its activities, fully or in part, on the territory of another Member State? If not, does the principle of effective access to justice impose a duty of cooperation between Member States' supervisory authorities?

15. The CJEU affirms, implicitly referring to the principle of effectiveness, that Directive no. 95/46 requires that each authority may be requested to exercise its powers by another Member State's authority and that the supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information. National supervisory authorities should cooperate. The authority to which the original complaint has been submitted must, in fulfilment of the duty of cooperation, request the supervisory authority of the Member State whose law is applicable, to establish whether there is an infringement of that law and to impose penalties if that law permits.

16. In *Holstein*, the CJEU decides that where the data protection authorities of two different Members States have joint competence in a case, as a result of the broad interpretation given to the concept of 'in the context of an establishment',

there is no hierarchy between them. More specifically, the competent supervisory authority of a Member State may assess the lawfulness of data processing without first calling on the supervisory authority of the Member State where the entity actually processing the data has it seat/ is established.

17. Question 4 - Which court has jurisdiction to order that wrongful data published on a website accessible in several Member States be rectified and/or removed?

18. Directive 95/46 included no rules regarding the jurisdiction of national courts. The CJEU relied on Regulations *Brussels I* and *I bis*, particularly on the rules of jurisdiction relating to matters of tort,, to offer data subjects access to the courts. In *Svensk Handel*, the Court implicitly relied on the principle of effective access to justice and the principle of proportionality – by balancing the claimant's interest in easily identifying the court in which he might sue with the defendant's interest in reasonably foreseeing the court in which he might be sued - to decide that a data subject whose personal rights have been infringed by data processing: 1) may bring a claim for compensation for the entire damage before the courts of the Member State where he/she/it has the centre of his/her/its interests; 2) may bring an action for rectification and/or removal of information only before the courts of each Member State in which the information published on the internet is or was accessible.

19. The GDPR creates a specific rule of jurisdiction for data subjects that will take precedence – where applicable – over the rules defined in Regulations *Brussels I/ Brussels I bis*. The GDPR recognises a "right to an effective judicial remedy against the controller or processor for the data subject whose rights have been infringed, and gives jurisdiction over the claims to "the courts of the Member State where the controller or processor has an establishment" or, alternatively, "before the courts of the Member State where the data subject has his or her residence".

20. **Questions 6 & 7 - Should Member States' data protection authorities assess the adequacy of data protection in third countries to which personal data gathered in the European Union is to be transferred, in terms of European Union principles and/or legislation? Should they find that the data protection offered in a third country is not adequate, should Member States oppose the transfer of personal data gathered in the European Union to that country?**

21. In *Schrems* the CJEU affirms, implicitly applying the principle of effectiveness, that if national supervisory authorities were not responsible for verifying whether a transfer of personal data to a third country complied with EU protection principles, data subjects "would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights". For the Court, it follows that the level of protection offered by the United States must be scrutinized according to EU standards, notably the principle of proportionality.

With regard to the generalised access by US authorities to personal data transferred from the EU, the CJEU observes that under US legislation, the violation of the right to respect for private life is not, as it should be, "limited to what is strictly necessary".

22. When it appears, from the assessment made by the Court or by national authorities and/or courts, that the level of protection in a third country is not sufficient, Member State supervisory authorities are required to oppose the transfer of personal data by a controller established in that Member State to another controller established in that third country where the processing of personal data is to be undertaken.

Impact of the Charter on the material scope of data protection

23. Notwithstanding the definitions, enshrined in article 2 of Directive 95/46, of concepts such as 'personal data, 'processing', or 'data subject' – concepts which are important for the delimitation of the scope of the protection - , questions and disputes have arisen regarding the precise meaning of such concepts.

24. Question 1 - In the light of the principle of effectiveness of data protection, how should the concept of "processing of personal data" be interpreted? In the light of the principle of effectiveness of data protection, how should the limits to the scope of the protection defined by EU legislation be implemented?

25. The Court implicitly relies on the principle of effectiveness in its jurisprudence to endorse a broad conception of the general scope of Directive 95/46. It is important to stress that the Court endorses a two-step reasoning. Firstly, it focuses on the "positive" material scope of the directive in the light of article 3 (1); and secondly, it verifies whether the disputed processing falls within the activities not covered by the protection, pursuant to article 3 (2) of the directive. In the latter case, the data subject would not be able to claim the protection afforded by the directive and/or national law.

26. In *Google Spain* and *Satamedia*, the Court endorses a broad conception of the general scope of the directive, stressing that not only does the wording of article 2 (b) of the directive require the inclusion of activities considered to fall within the meaning of "processing of data", but also that "a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect". However, in *Lindqvist*, the Court mitigates the consequences of the principle of effectiveness and contains the scope of the directive within reasonable limits, implicitly referring to the principle of proportionality. Even if Member States may extend the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope of that directive, measures taken by the Member States to ensure the protection of personal data should be consistent with the directive's objective of maintaining a

balance between the free movement of personal data and the protection of private life.

27. Question 2 – In the light of the principle of effectiveness of data protection, how should the concept of "personal data" be interpreted?

28. In *Breyer*, the CJEU relies on the principle of effectiveness to decide that, within the meaning of article 2 of Directive 95/46, 'personal data' refers not only to information which actually permits the identification of a person, but also to each piece of information which, even though not in itself allowing such identification, could allow such identification if combined with other pieces of information. Moreover, the Court judges that there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. In *Nowak*, the Court confirms that 'personal data' relates not only to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.

29. Question 3 - In the light of the principle of effectiveness of data protection, how should the concept of "controller" of the processing of personal data be interpreted?

30. In *Google Spain*, the CJEU clearly builds on **the principle of effectiveness** to promote a broad definition of the concept of 'controller' within the meaning of the directive, so that the operator of a search engine is included in this definition. Analyzing the concrete role played by the operator of a search engine, the Court observes firstly that it determines the purposes and means of its activity, and secondly that such activity can be distinguished from, and is additional to, that carried out by publishers of websites. The Court concludes that it "would be contrary, not only to the clear wording of article 2 (d) of the directive 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" (§34).

31. In *Holstein* and *Jehovah*, based on the objective of ensuring effective and complete protection to data subjects, the Court raises the issue of joint responsibility in relation to the processing of data. Recalling that pursuant to article 2 (d) of Directive 95/46, the concept of controller may cover several actors taking part in the processing, the Court concludes that a party is a controller as long as it contributes to the processing by taking part in the determination of the purposes and means of processing the personal data. The existence of joint responsibility does not necessarily imply equal responsibility or involvement in the processing, nor equal access to the personal data.

32. Question 4 - In the light of the principle of effectiveness of data protection, how should the concept of "data subject" be interpreted?

33. National case law has addressed in more detail the question of who, precisely, is the holder of the rights laid down by EU legislation with regard to data protection.

34. The French *Conseil d'Etat* observes that the right to access is available only with regard to the personal data of the person exercising the right. Successors or assignees of the person to whom the personal data relates, such as heirs, cannot be automatically assimilated to such person. However, when a person who suffers damage dies, his right to compensation is transmitted to his heirs, who replace him in pending legal actions brought to seek compensation for the damage suffered. Therefore, heirs should be classified as "persons to whom personal data relates" for the purpose of exercising the deceased's right to access, insofar as the data to which access is sought is necessary for the purpose of pursuing the action for compensation.

35. Question 5 – In the light of the principles of effectiveness and proportionality, to what extent may data subjects' rights to the protection of private life and personal data (articles 7 & 8 of the Charter) be limited by Member States for the purpose of protecting public security, defence or State security?

36. In *Digital Rights Ireland*, the CJEU examines interference with data protection in the light of Article 52(1) CFR. It recognizes that interference may satisfy an objective of general interest, since the material objective of Directive 2006/24 is to contribute to the fight against serious crime and thus, ultimately, to public security. The Court then engages in the evaluation of the interference in the light of the principle of proportionality: after finding that data is a valuable tool in pursuing the objective, so that retention of such data may be seen as an appropriate measure for attaining that objective, it states that given the importance of the fundamental rights at stake, EU legislation must lay down clear and precise rules governing the scope and application of the measure and impose minimum safeguards so that the persons whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. But Directive 2006/24 does not lay down any such clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

Impact of the Charter on the assessment of the legitimacy of data processing

37. The right to the protection of data, laid down by EU secondary legislation, may come into conflict with other legitimate interests. The fundamental rights of data subjects where data protection is concerned are, particularly, the right to

privacy, protected by article 7 of the Charter, and the right to the protection of personal data, covered by article 8 of the Charter.

38. Question 1 - In the light of the principle of effectiveness and proportionality, to what extent may data subjects' rights to the protection of private life and personal data (articles 7 & 8 of the Charter) be limited by Member States because they are in conflict with other legitimate private interests of the controller or a third party, including fundamental rights?

39. In *Promusicae*, the CJEU affirms that Directive 2002/58 does not preclude Member States from laying down, with a view to ensuring effective protection of copyright, an obligation to communicate personal data that will enable the copyright holder to bring civil proceedings based on the existence of that right. The Court observes that Article 15(1) of Directive 2002/58 authorises the Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary, inter alia, for the protection of the rights and freedoms of others, which include the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings.

40. The CJEU then assesses the potential conflict between property rights, the right to effective judicial protection and right to data protection. To reconcile the requirements of the protection of these fundamental rights, the Court urges the Member States to transpose and implement directives so to avoid any conflict of fundamental rights. If such a conflict cannot be avoided, in the view of the Court, Member States should rely on general EU principles, in particular the principle of proportionality, to reach a balanced solution that will not unduly sacrifice the effective protection of one fundamental right for the protection of another (principle of effectiveness).

41. Accordingly the CJEU provides a set of criteria to be weighed in the balance by national courts: the duration of the breach of data protection; the importance, for the persons concerned, of protecting the data disclosed; the fact that the data in question already appears in public sources; the nature of the information in question and its sensitivity for the data subject's private life; the public interest in the information; and the age of the data subject.

Effective Data protection between administrative and judicial enforcement

42. To ensure efficient protection of personal data, the European Union relies mainly on national supervisory authorities. The role of judicial enforcement should not, however, be underestimated, and the directive lays down the "right to a judicial remedy" for any person who has suffered damage as a result of an unlawful processing operation. Still, the role of judicial enforcement seems to vary between the Member States. The coexistence of administrative enforcement, conducted by national supervisory authorities, and judicial enforcement, raises important issues such as that of the coordination of both types of proceedings.

The Charter and/or the principles of effectiveness, proportionality and dissuasiveness may provide solutions to such issues.

43. Question 1 – In data protection cases, what is the role of the right to an effective judicial remedy in defining the relationship between administrative and judicial enforcement?

44. The possible relationships between administrative and judicial enforcement on the basis of current legislation are the following: (a) Alternative; (b) Complementary with simultaneous or sequential procedures; (c) Independent.

45. In *Puskar*, the Court points out that the obligation to exhaust additional administrative remedies must be scrutinized in the light of article 47 CFREU, article 4 (3) TEU, and article 19 (1) TEU. Such an obligation to exhaust additional administrative remedies constitutes a limitation on the right to an effective judicial remedy. Therefore, it can be justified, according to the criteria laid down in accordance with article 52 (1) CFREU, only where:

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.

46. As regards the existence of objectives of general interest, the Court acknowledges 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 which can be decided in a shorter time before 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 pursues objectives of general interest.

47. As regards the proportionality test, the CJEU adopts the reasoning in *Alassini*:

- The procedures do not result in a decision which is binding on the parties,
- The procedures do not cause a substantial delay for the purposes of bringing legal proceedings
- The procedures suspend the period for the time-barring of claims
- The procedures do not give rise to costs — or give rise to very low costs — for the parties
- Electronic means are not the only means by which the settlement procedure may be accessed and
- The procedures allow for interim measures in exceptional cases where the urgency of the situation so requires.

48. Question 3 - 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?

49. Where there is a Commission decision regarding the existence of an adequate level of protection of personal data, national supervisory authorities and courts are bound by the decision of the Commission. However, the Court acknowledges that it would be contrary to the system laid down in Directive 95/46, and implicitly contrary to the right to an effective remedy, if national supervisory authorities could not examine a claim brought by a data subject concerning the protection of his rights and freedoms with regard to the processing of his personal data that had been or could be transferred from a Member State to the third country covered by that decision.

50. Question 4 – Is the supervisory authority of a Member State able to examine the claim of a person that questions the validity of an EU act?

51. If an individual presents a claim before the national supervisory authority alleging the incompatibility of an EU act with fundamental rights and freedoms, and the national supervisory authority concludes that the claim is unfounded, then the claimant should, pursuant to article 28(3) of Directive 95/46 read in the 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 rights and freedoms, they must present a preliminary reference to the CJEU.

52. If an individual presents a claim before the national supervisory authority alleging the incompatibility of a EU act with fundamental rights and freedoms, and the national supervisory authority concludes that the claim is founded, then the supervisory authority must, pursuant to article 28(3) of Directive 95/46 read in the light in particular of article 8(3) CFREU, be able to institute legal proceedings. In such 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 ask for a preliminary ruling for the purpose of examination of the decision's validity.

53. Questions 5 & 6 – What are the powers of courts in their judicial review of administrative decisions? When the national systems envisage two alternative procedures, in which the national supervisory authorities decide on the violation of data protection law, and the courts determine the damages, are the courts bound by administrative decisions in terms of (a) the existence of the violation; (b) the use and acquisition of (new) evidence; and (c) the type and content of the penalty? If they are not bound, what legal effect do administrative decisions have on the judicial remedies?

54. In the *East Sussex Council* case, outside the field of data protection, the CJEU affirmed that where the European legislation does not specify the scope of

judicial review, it is for the legal systems of the MS to determine that scope, subject to the principles of equivalence and effectiveness.

55. This is confirmed by national case law. In Italy, first instance courts, performing the function of judicial review, are not bound by the decisions of national supervisory authorities either in terms of the existence of the violation, or on the use and acquisition of (new) evidence, or on the type and content of the penalty. In a different case, the Italian Supreme court addressed the impact of the decision of the national supervisory authority on the judicial proceedings concerning damages. Given that the decision of the court may also be handed down in a different proceeding at a later date than the claim before the national supervisory authority for breach of data protection rules, the Supreme Court affirmed that the decision of the supervisory authority cannot bind the civil court. As such, a decision will never acquire the status (or have the effects) of res judicata, due to the fact that the data protection authority is an administrative body, and its procedure guarantees the impartiality of the data protection authority as does the procedure of a court in a legal proceeding.

Impact of the Charter on the conduct of proceedings

56. The right to the protection of data may be argued in order to prevent the production of evidence in court, when it is claimed that the piece of evidence infringes the right to the protection of personal data. The CJEU relies, again, on a balance between two fundamental rights – the right to a fair hearing, and the right to the protection of data – to define the methodology that national authorities should implement when facing such a situation.

57. Question 1 - Should a document including personal data, which has been rendered inaccessible to prevent unauthorized disclosure, be regarded as lawful evidence of the existence of the allegedly unlawful processing of such data when produced by an unauthorized person, with the result that the referring court may admit this evidence in accordance with the requirements of EU law on a fair hearing found in the second paragraph of Article 47(2) of the Charter?

58. In *Puskar*, the Court affirms that the rejection of a list as evidence of an infringement of the rights conferred by Directive 95/46 constitutes a limitation on the right to an effective remedy before a court. The Court looks to the factual circumstances of the case in order to verify whether the rejection affects the essential content of the fundamental right to effective judicial protection. If the piece of evidence is relevant and crucial to the claimant's cause, such rejection can be found disproportionate.

59. The purpose of protecting the right of the persons whose data appears in these documents might justify a refusal to allow the unauthorized internal documents to be produced in judicial proceedings. However the Court stresses that the referring court should ascertain whether or not such a rejection

disproportionately affects the right to an effective remedy before a court, referred to in article 47 of the Charter.

60. Question 2 - In the light of the right to a fair hearing laid down in article 47 (2) of the Charter, can evidence obtained through the unlawful processing of data be produced and used in court?

61. The jurisprudence of the CJEU shows that when the processing of data does not fall under one of the derogations from data protection admitted by law, judges should rely on the principle of proportionality to balance the right to protection of private life and data protection of the data subject against the conflicting rights of the controller. For instance in *Ryneš,* the Court invited national authorities, in the implementation of national law, to balance the right to data protection and privacy with the legitimate interests of the controller in protecting his home and family. The same reasoning could apply to balance the right of the controller to effective access to justice, which is at stake where the admissibility of evidence is in issue, with the rights of the data subject, taking into account whether the use of the data is a decisive factor on which the conviction of the defendants depends.

Effective, proportionate and dissuasive sanctions and remedies

62. The effective protection of natural persons in relation to the processing of personal data calls for effective and dissuasive sanctions and remedies against infringers of the data subjects' rights.

63. Question 1 - In order to ensure an effective remedy for data subjects, should EU law be interpreted as implicitly including a right to be de-listed, so that data subjects may obtain orders against controllers to oblige them to remove, from the list of results displayed by search engines, links to web pages published by third parties, even where the data available - the publication of which was lawful – has not previously or simultaneously been erased from those web pages?

64. In *Google Spain*, the CJEU affirms that data subjects have the right to obtain from the controller the rectification, erasure or blocking of data processing which does not comply with EU legislation, "in particular" because that data is incomplete or inaccurate. This should be the case where the processing of data is inadequate, irrelevant or excessive in relation to the purposes for which it are collected and/or processed, and when the balance of interests is weighted in favour of the data subject's right to privacy and protection of data.

65. The Court thus concludes that supervisory or judicial authorities may order the search engine to de-list the results, on the basis of the principle of effectiveness, since 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".

66. The material scope of the right to be de-listed calls for further clarification. The issue has been raised by the French *Conseil d'Etat*, concerning press articles containing sensitive information. Similar doubts have been raised about the territorial scope of the right to be de-listed.

67. National case law shows that courts have difficulties in striking a balance between freedom of expression and data protection. The French case law, after *Google Spain*, tends to examine the interests involved, weighing the legitimate interest of the public to access the information published and referenced, with the right of data subjects to data protection. For this purpose, courts examine the veracity, the date of publication, the intimacy and the prejudicial aspects of the personal data disclosed.

68. Question 2 - In order to ensure the effective protection of personal data within the European Union and full compensation of victims, should courts award compensation for material and non-material damage for any infringement of EU data protection law regardless of whether any specific harm has been caused by the infringement?

69. National jurisprudence offers examples of the relationship between the principle of solidarity and the principle of effectiveness of fundamental rights. Indeed, the effective protection of these rights becomes sustainable within society only if the infringement is serious and the consequences are not trivial.

70. The Italian Supreme Court argues that non-economic losses may be recovered, provided that fundamental rights are violated or the law expressly allows for recovery of non-economic losses, only if the infringement is serious and the damages are not trivial. Moreover, the court highlights the distinct role of injunctions and damages and the possibility of a modular enforcement in which the remedial response is adjusted to the material needs of protection of the victim. Whereas injunctions mainly have a preventive function, damages will be used only if prejudice is concrete, effective and substantial.

71. In *EDPS v European Parliament*, the EU Civil Service Tribunal addresses the question whether the annulment of an act of the Parliament may in itself constitute appropriate and, in principle, sufficient reparation for non-material damage and, if not, how non-material damage should be assessed. The Tribunal concludes that the annulment of the administration's unlawful act cannot constitute full reparation for the non-material damage: (i) if that act contains an assessment of the abilities and conduct of the person concerned which is capable of offending him; (ii) where the illegality committed is particularly serious; and (iii) where the annulment of an act has no practical effect.

72. Question 3 - Should a court or supervisory authority, with which an aggregated complaint has been lodged by an individual also vested with a mandate by multiple claimants, extend to the whole group of claimants, under the principle of effectiveness, the type of protection assigned by law to the individual by virtue of his status as a consumer, e.g. with regard to the place of jurisdiction?

73. The issue of collective redress in the implementation of EU legislation on data protection has not been directly addressed by the CJEU, mainly because Member States have not yet, or have only very recently, adopted national legislation allowing for collective action against infringers of data protection.

74. In *Schrems II*, the CJEU had to decide whether a consumer within the meaning of Regulation Brussels I/Ibis could bring, before the courts of his own domicile, at the same time as his own claims arising from a consumer supply, the claims of other consumers domiciled: a) in the same Member State, b) in another Member State, or c) in a non-Member State. The Court affirms that article 16 of the Brussels regulation does not apply to collective claims. However, this does not exclude the possibility of coordinating the claims of multiple victims in collective redress procedures in the field of data protection.

75. Article 80 GDPR deals with representation of data subjects before supervisory authorities and courts. This provision does not necessarily deal with collective redress, since the mandate of the body, organisation or association may remain individual and must be dealt with as such.

76. If article 80 were interpreted as also covering collective claims for redress, the question arises whether this type of aggregation should be favoured from the standpoint of effective protection of data subjects, given the greater capacity of this type of institution to coordinate multiple claims, to identify potentially interested victims, to lower the costs of litigation, and therefore to increase the deterrent effect of the enforcement mechanisms.

77. Question 4 - In order to ensure the effective protection of personal data within the European Union, can national data protection authorities exercise powers that are not expressly conferred upon them by EU Law?

78. In *Weltimmo*, the CJEU stresses that the list of national supervisory powers provided by article 28 of Directive 95/46 should not be seen as exhaustive, and that given the type of powers of intervention mentioned in that provision, those powers of intervention should be taken to include the power to penalise the data controller by imposing a fine on him, where appropriate. The decision relies on the principle of effectiveness, since the reasoning of the Court is based on the idea that, since national supervisory authorities are established to ensure compliance with the regulation on data protection, they should be vested with the necessary powers to do so, even if such powers are not expressly listed in Directive 95/46.

79. Question 5 - What is or should be the impact of the principles of proportionality and/or dissuasiveness on the definition and/or implementation of sanctions and remedies for violations of data protection?

80. In *Lindqvist*, the CJEU addresses the issue of the proportionality of the sanction, affirming that the protection of private life requires the application of effective sanctions against people processing personal data in ways inconsistent with Directive 95/46, but that such sanctions must always respect the principle of proportionality. The Court points to the following criteria for assessing proportionality: the duration of the breach and the importance, for the persons concerned, of the protection of the data disclosed.

81. The Court thus puts in perspective both principles, of effectiveness and proportionality, which should be considered together when imposing a sanction. Sanctions have to be effective, but they should not be disproportionate. And national courts or authorities should take into account all the circumstances of the case in order to assess what should be the appropriate sanction.

82. National jurisprudence provides examples of such a balance. For instance, the French *Conseil d'Etat* observes that when the French supervisory authority imposes, in addition to the main sanction, a measure consisting of publicizing the sanction imposed on the controller, such an additional sanction is necessarily subject to the principle of proportionality, even if the law does not expressly state as much. The lawfulness of the sanction should be assessed, in particular, in the light of the type of publishing medium, and of the time for which the publication is available to the public.

83. Question 6 - In order to ensure the effective protection of personal data within the European Union, to what extent may the sanctions and remedies applicable to consumer protection be transposed to the protection of data subjects?

84. In *Amazon*, the CJEU does not agree that the protection of data subjects can be extended through the application of the rules on consumer protection. When data processing is encompassed in a consumer contract, the question whether such data processing is lawful shall be governed only by the law of the Member State where the controller's establishment, in the context of the activities of which the data processing is carried out, is located, pursuant to article 4 of Directive 95/46. The law of a Member State to which the seller/controller directs its commercial activities, applicable to the consumer contract pursuant to Regulation Rome I, may not apply in assessing the lawfulness of the processing of data obtained under such a contract, unless it is also the law of the Member State where the establishment is located in the context of the activities of which the data processing is carried out.

85. However, the principle of effectiveness and dissuasiveness may point to a different result: it may be more effective and dissuasive to allow the victim to choose between two national regimes, to select the one that imposes heavier sanctions on the infringer.

86. As regards the interplay between data protection and consumer protection, in *Schrems II*, the CJEU affirms that when the processing of data is encompassed in a consumer contract, the data subject is also a consumer. The data subject may therefore rely, to identify the courts having jurisdiction over his claims against the other party/controller, on the rules for the protection of consumers in the Brussels I Regulation; however, the law applicable when assessing the lawfulness of the processing of data is necessarily the law of the Member State where the establishment is located in the context of the activities of which the processing is carried out, within the meaning of Directive 95/46. The law governing the consumer contract is not applicable to such assessment.