FIDE 2021 Congress - Topic 2: EU Data Protection Law: An Update

As in politics, a year is a long time in EU data protection law. Since the submission for publication of the general and institutional reports in early 2020, there have been several significant judgments delivered by this Court regarding the topics covered in these reports and there are important preliminary references pending before it. National Supervisory Authorities (NSAs) have made approximately 600 further decisions, including a record fine of €775 million addressed to Amazon by the Luxembourgish NSA.

Moreover, beyond the topics covered in the original reports (which concerned the development of data protection law at national level), the pandemic itself tested the effectiveness of the EU data protection regime when Member States sought to rely on technological fixes to address the health and societal challenges it entails. Meanwhile, the European Commission continues to propose new legislative initiatives, most notably the proposed AI Act, which like other pending initiatives would fundamentally alter the regulatory context in which the GDPR applies.

A thorough examination of all of these developments is not possible. Rather, in advance of the 2021 Congress meeting, this update seeks simply to highlight some of the more significant elements. Part I considers notable developments relating to the topics covered in the original reports while Part II reflects on the wider role of the GDPR in the context of the pandemic and recent regulatory developments.

I. Relevant Developments on Report Topics

The FIDE questionnaire sub-divided the questions for National Rapporteurs into four sub-topics, which shall be used to structure this update.

1. Setting the Scene – Testing the Flexibility Afforded by the GDPR

As a Regulation, one might expect the uniform reception of the GDPR into national legal orders. However, as is well-documented, the GDPR affords Member States some flexibility to tailor its application to the national legal and societal context. For instance, Article 23 GDPR enables Member States to introduce legislative measures to restrict the scope of the rights provided for in Articles 12 to 22 (and the corresponding obligations in Article 5) as well as Article 34. It provides a list of legitimate interests that such a restriction may pursue and requires that any such restriction respect the essence of relevant fundamental rights and be necessary and proportionate. In *VQ v Land Hessen*[1], the Court was required to consider whether the activities of the Petitions Committee of the Parliament of the *Land* Hessen fell within the material scope of the GDPR. The Court found that none of the derogations from the scope of the GDPR in Article 2 were applicable but also that Article 23 GDPR (and the accompanying recital 20) contain no exception for parliamentary activities.[2] The Court therefore treated the legitimate interests specified in Article 23 GDPR as an exhaustive list.

The facts of *Latvijas Republikas Saeima*[3] provide a good illustration of an aspect of EU data protection law where Member States have been afforded less flexibility by the GDPR than under its predecessor the 1995 Data Protection Directive. Article 10 GDPR concerns the processing of personal data "relating

*This update was authored by Anna Buchta and Herke Kranenborg (Institutional Rapporteurs) and Orla Lynskey (General Rapporteur). The opinions expressed in the report reflect the authors' personal opinions and cannot be attributed to the EDPS or the European Commission.

[1] Case C-272/19 *VQ v Land Hessen* EU:C:2020:535.

[2] Ibid, paras 71 and 72.

[3] Case C-439/19, Latvijas Republikas Saeima (Points de pénalité) EU:C:2021:504

to criminal convictions and offences". The Latvian Constitutional Court asked the CJEU whether the term "criminal convictions and offences or related security measures" found in Article 10 GDPR includes personal data processing relating to penalty points for motoring offences. Such motoring offences are classified as administrative offences by domestic law. The Court held that the term "criminal convictions and offences" refers exclusively to criminal offences. To justify this finding, it pointed to the legislative history of the provision; while the European Parliament had proposed the inclusion of the wording "administrative sanctions" this wording was not reflected in the final text. The Court concluded that:

> in deliberately not including the adjective 'administrative' in Article 10 of the GDPR, the EU legislature intended to limit the enhanced protection provided for by that provision to the criminal field alone.[4]

The Court also noted that this represented a change from the 1995 Directive which referred to the "processing of data relating to offences, criminal convictions or security measures" and which stated further that Member States "may provide that data relating to administrative sanctions…shall also be processed under the control of official authority". It is therefore apparent that the possibility for Member States to apply this provision to all administrative offences is now foreclosed by the GDPR. Only administrative offences that might be categorised as criminal fall within its ambit.

Whether the GDPR precludes the more restrictive interpretation of some of its provisions by Member States will be tested in a pending referral before the Court.[5] The Court is asked to confirm the meaning of Article 38(3) GDPR. This provision states that a Data Protection Officer (DPO) "shall not be dismissed or penalised by the controller or the processor for performing his tasks". The European Data Protection Board (EDPB) understands this provision to mean that the DPO can nonetheless be dismissed for other reasons, unrelated to the performance of their tasks (for instance, sexual misconduct).[6] German law prohibits the ordinary termination of the DPO's employment contract, irrespective of whether this dismissal is related to the performance of the tasks of the DPO. In this respect, the German law is stricter than the interpretation proposed by the EDPB, offering better protection to the position of the DPO. However, on this point the GDPR does not indicate that the Member State may add such stricter requirements. The Court is therefore asked whether the GDPR precludes such a domestic law prohibition.[7]

The Court is also asked to consider whether this finding extends to situations where the designation of a DPO is not mandatory pursuant to Article 37(1) GDPR. Initially this latter element might seem to resemble a *renvoi* situation, where national legislation adopts the same approach as that adopted in an EU measure and the Court thus accepts jurisdiction to interpret these purely domestic law provisions. However,
Article 37(4) GDPR enables data controllers, processors and Member States to require the designation of DPOs in other circumstances. The referring court therefore simply wishes to know whether this interpretation of Article 38(3) GDPR applies also in these circumstances.

2. The Reception of Substantive GDPR Provisions in the National Legal Order

[4] Ibid, para 78.
[5] C-534/20, *Leistritz AG v LH*.
[6] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPOs)" WP 243 rev.01, revised and adopted on 5 April 2017 (as endorsed by the European Data Protection Board (EDPB), p. 15 and 16.
7 The precise wording of the question is as follows: "Is the second sentence of Article 38(3) GDPR based on a sufficient enabling clause, in particular in so far as this covers data protection officers that are party to an employment contract with the data controller?". See also the pending questions in Case C-453/21, X-FAB Dresden GmbH & Co. KG.

The Court has had the opportunity to clarify the interpretation of a number of key GDPR provisions in its recent jurisprudence.

(a) Valid consent

In *Orange Romania*[8] the Romanian NSA issued an administrative penalty to Orange Romania, a mobile telecommunications service provider, for having taken and retained copies of customer identity documents without their valid consent.

It was Orange Romania's practice when concluding paper-based contracts with individual customers for its mobile telecommunications services to annex copies of their identity documents to these contracts. The consumer contracts indicated that the customer had been informed of this collection and storage by Orange Romania and that the existence of customer consent was established by the insertion of crosses in boxes in the written documentation evidencing the contract. The relevant segment of the clause in question stated: "he or she [the customer] has been informed of, and has consented to, the following: the storage of copies of documents containing personal data for identification purposes". It was an Orange Romania agent that completed this tickbox on the retention of an identity document (usually on a computer) before customers signed to accept all of the contractual clauses.[9] That representative should also have informed the customer that this checkbox did not need to be ticked. Moreover, Orange Romania contined to conclude subscription contracts with customers who refused to consent to the storage of a copy of one of their identity documents. However, where a customer refused to provide consent, and thus wanted to deviate from this standard contract, Orange Romania required the customer to document this on the contract in handwriting in accordance with its internal procedures.

The Court was asked to provide guidance on whether such a practice and contractual clauses meet the requirements to demonstrate that a person's consent is validly given.[10]

The Court affirmed, in general terms, the requirements for consent found in EU data protection law. Consent must be active as now explicitly specified in the GDPR.[11] Consent must also be specific "in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes".[12] The Court noted that Article 7(2) GDPR requires that where consent is sought in the context of a written declaration that also concerns other matters, that consent request should be presented in a clearly distinguishable way from the other matters. Moreover, informed consent requires that the consent declaration must be presented in an intelligible and easily accessible form, using clear and plain language, particularly for pre-formulated declarations of consent. The information provided should enable the data subject to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. Freely given consent requires that the contractual terms must not mislead the data subject as to the possibility of concluding the contract even if they refuse to consent to the processing of their data.

[8] Case C-61/19, *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* EU:C:2020:901.
[9] Ibid, para 45.
[10] Ibid, para 33.
[11] Ibid, para 36.
[12] Ibid, para 38.

The Court then turned to consider how these criteria applied to the contractual clauses under consideration. As an Orange Romania agent ticked the checkbox prior to the customer signing the contractual clauses the Court held that "the mere fact that that box was ticked is not such as to establish a positive indication of those customers' consent to a copy of their identity card being collected and stored."[13] This tick-box, without more, did not prove that the clause was actually "read and digested". The Court left it to the referring court to investigate whether this was the case.

The Court noted that the ticked clause in question did not appear to have been presented in a clearly distinguishable manner from other contractual clauses, putting in doubt its specificity.[14] The Court also considered that further investigation was required to assess whether consent was informed, in particular whether the clauses were capable of misleading the data subject as to the possibility to conclude the contract without giving consent.[15] The Advocate General had been more definitive on this point, noting that it was not "made crystal-clear to the customer that a refusal to the copying and storing of his or her ID card does not make the conclusion of a contract impossible".[16]

The Court considered, like the Advocate General, that the free nature of the consent also appeared to be called into question. The Advocate General had opined that consent could not be freely given as customers who declined to consent were put in a situation where they "perceptibly deviate from a regular procedure".[17]

Finally, both the Court and the Advocate General noted that it is for Orange Romania, as the data controller, to establish that its customers have actively given their consent to the personal data processing. According to the Court this precludes the possibility of Orange Romania requiring customers actively to express their refusal.[18]

(b) Legitimate interests

In the case of *TK v Asociaţia de Proprietari bloc M5A-ScaraA*[19], the Court had the opportunity to consider the application of the legitimate interests legal basis in the context of CCTV video recording. TK lived in a building where the association of building co-owners had installed a video camera surveillance system in some common parts of the building following a collective decision at a general assembly. One of these cameras was directed towards the front of the building while another two cameras were in the ground-floor hallway and in the lift. TK initiated proceedings against the association in order to have the cameras removed. These cameras had been installed in response to a number of criminal episodes in the building given that other security mechanisms (such as the installation of an intercom and magnetic card entry system) had been unsuccessful.

In its preliminary reference, the national court queried whether Articles 8 and 52 EU Charter and Article 7(f) of the 1995 Directive preclude national legislation that allows video surveillance to be used without the data subject's consent to ensure the safety and protection of individuals, property and valuables.[20]

[13] Ibid, para 46.
[14] Ibid, para 47.
[15] Ibid, para 49.
[16] Opinion of the Advocate General in Case C-61/19, *Orange Romania SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* EU:C:2020:901, para 61.
[17] Ibid, para 60.
[18] *Orange Romania* (n 8), para 51.
[19] Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064.
[20] Ibid, para 32.

In particular, the referring court asked whether the legitimate interests of a controller must be "proven" and be "present and effective at the time of the data processing".[21]

Several states and the Commission had intervened before the Court to argue that the legitimate interests must be present and effective as at the date of the data processing and must not be hypothetical at that date, while acknowlesfing that this does not necessarily mean that the safety of property had already been compromised at the time of processing. The Court noted that the requirement of present and effective interest appeared to be fulfilled in this case as thefts, burglaries and vandalism had already occurred before the video surveillance system was installed.

Concerning the necessity of personal data processing to pursue these legitimate interests, the Court has held that derogations and limitations "in relation to the protection of personal data must apply only in so far as is strictly necessary". According to the Court, this means that the objective pursued cannot reasonably be as effectively achieved by other means less restrictive of fundamental rights.[22] In considering the need for processing, the Court also affirmed that this assessment must be made in conjunction with the data minimisation principle, according to which personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".[23]

The Court considered that the proportionality of the measures had been taken into account by the data controllers. Alternative security measures had been enacted but were insufficient, and the camera surveillance system was limited to particular parts of the building. Nevertheless, the Court endorsed the Commission's contention that in assessing whether such processing is necessary, the controller must examine "whether it is sufficient that the video surveillance operates only at night or outside normal working hours, and block or obsecure the images taken in areas where surveillance is unnecessary".[24]

With regard to the balancing of rights entailed by the third limb of Article 7(f), the Court reiterated that this balancing will depend on the individual circumstances of a particular case and that account must be taken of the significance of a data subject's EU Charter rights. It specified that this precludes Member States from

> excluding, categorically and in general, the possibility of processing certain categories of personal data without allowsing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.[25]

The Court noted that the seriousness of the infringement of the data subject's fundamental rights might vary depending on whether the data concerned came from a public or non-public source. It held that the processing of data from non-public sources involved a more serious infringement of the rights to data protection and privacy as it implies that "information relating to the data subject's private life will thereafter be known by the data controller" as well as third parties to whom it may be disclosed. The Court reiterated some of the criteria relevant to this balancing exercise that it had previously identified in its case law. It concluded that the principle of data minimisation and the legitimate interests legal

[21] Ibid, para 43.
[22] Ibid, para 47.
[23] Ibid, para 48.
[24] Ibid, para 51.
[25] Ibid, para 53.

basis do not preclude national provisions such as those in the main proceedings, provided that the personal data processing fulfils the conditions laid down in Article 7(f).

The facts of *M.I.C.M*[26] replicate those of the earlier *Promusicae*[27] judgment. Miricom is a copyright holder which holds rights over content (in this instance pornographic films). It had relied on a third party to gather the IP addresses of those who were infringing its copyright on peer-to-peer networks using the BitTorrent protocol. Telenet, a Belgian Internet Service Provider (ISP) refused to provide Miricom with information identifying the account holders linked to the infringing IP addresses. Amongst the issues the Court was asked to provide guidance on was the question of whether Miricom could rely on Article 6(1)(f) GDPR to collect the relevant IP addresses. In particular, the Court interpreted the question it was asked as follows: whether Article 6(1)(f) GDPR

> must be interpreted as precluding, first, the systematic registration, by the holder of intellectual property rights and by a third party acting on that holder's behalf, of the IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities and, second, the communication of the names and of postal addresses of those users to the rightholder or to a third party in order to enable him or her to bring a claim for damages before a civil court for prejudice allegedly caused by those users.[28]

The Court confirmed that the registration of IP addresses constitutes personal data processing. On the application of Article 6(1)(f), it affirmed that as the relevant provisions of the GDPR have "essentially the same scope" as the relevant provisions of the 1995 Directive, the Court's case-law on the Directive is in principle also applicable to the GDPR.[29]

The Court recognised that the recovery of claims by an assignee may constitute a legitimate interest.[30] It considered that the necessity criterion was likely fulfilled as it is often only possible to identify the owner of the interent connection on the basis of their IP address and the information provided by the ISP.[31] On the third limb of the legitimate interests test, the Court deployed the same reasoning as it had in its earlier caselaw under the Directive. This entailed an assessment of additional relevant legal obligations. It confirmed that a reading of Article 8(3) of the Directive on the Enforcement of IPRs in conjunction with Article 15(1) of the E-Privacy Directive and the (then) Article 7(f) of the 1995 Directive does not preclude Member States from imposing an obligation on data controllers to disclose data to private persons in order to enable them to bring civil proceedings for copyright infringements but nor does it require those Member States to lay down such an obligation.[32]

It advised the national court that if it were to follow from its investigations that domestic legislative provisions exist that limits the scope of the rights to privacy found in Article 5 and 6 of the E-Privacy Directive, if Miricom had legal standing to bring proceedings and if the request for information was proportionate and not abusive, then it would be lawful in accordance with the GDPR.[33]

(c) Additional Article 5 and 6 Jurisprudence

---

[26] Case C- 597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited v Telenet BVBA* EU:C:2021:492.
[27] Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU* EU:C:2008:54.

[28] Ibid, para 101.
[29] Ibid, para 107.
[30] Ibid, paras 108 and 109.
[31] Ibid, para 110.
[32] Ibid, para 125.
[33] Ibid, para 131.

In *Latvijas Republikas Saeima* the referring Court had queried whether the Article 5(1)(f) GDPR principle of "integrity and confidentiality" prohibited Member States from treating penalty points information about drivers as within the public domain and allowing for its further communication (without additional qualification). The Court extrapolated from the (precisely worded) questions of the national court that it seeks to establish whether the relevant processing was generally lawful in light of all of the provisions of the GDPR, in particular the principle of proportionality.[34] The Court therefore focused on the principle of data minimisation (Article 5(1)(c) GDPR) which "gives expression to the principle of proportionality".[35]

It began by noting that compatibility with the GDPR needs to be assessed both in light of general rules on legality, here Article 5(1)(c) and Article 6(1)(e), and the specific rules, here Article 10 GDPR. Article 6(1)(e) permits processing to the extent 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. The Court affirmed that none of these provisions impose a general and absolute prohibition on such disclosures by public authorities. The Court recalls that the EU Charter rights to data protection and to respect for private life are not absolute and that they must be considered "in relation to their function in society and be weighed against other fundamental rights". This entails an assessment under Article 52(1) EU Charter of whether the interference with these rights, taking into account its seriousness, can be considered justified and proportionate.

Having rooted its reasoning in the EU Charter, the Court then proceeded to conduct a proportionality analysis based on the specific provisions of the GDPR. While recognising that road safety improvement serves a public interest, it stated that the disclosure of penalty point data must be necessary to meet this objective. This necessity criterion is not met where the objective could be pursued just as effectively by other less restrictive means. It considered that this necessity test had not been met given that there was no indication that alternative less restrictive measures had been considered and that the disclosure of penalty point information constitutes a serious interference with relevant fundamental rights since it may "give rise to social disapproval and result in the stigmatisation of the data subject".[36] Moreover, these measures went beyond what was necessary because, amongst other things, they concerned the data of those who committed offences occasionally in addition to those who systematically disregarded the road traffic rules.

The Court is asked for guidance on the identification of the most appropriate legal basis for data processing in a number of pending preliminary references.

In an anticipated preliminary reference from a regional appeal court in Germany, the Court is asked to provide guidance on Facebook's practice of processing personal data obtained from third-party websites and applications and other Facebook group services.[37] At issue in the domestic proceedings was whether this practice had a valid legal basis. The CJEU is asked to clarify whether, when such personal data is used for the provision of personalised content and advertising, the Article 6(1)(b) "contractual necessity" legal basis or the Article 6(1)(f) "legitimate interests" legal basis might be used. As consent must be freely given, the Court is also asked whether consent can be freely and effectively expressed where the data controller is a dominant undertaking (pursuant to competition law).

[34] Latvijas Republikas Saeima (Points de pénalité) (n 3 above), para 97.
[35] Ibid, para 98.
[36] Ibid, para 113.
[37] Case C-252/21, *Facebook Inc. and Others v Bundeskartellamt.*

In a case taken by data protection activist Max Schrems against Facebook Ireland pending before the Austrian courts, the Austrian Court has referred a similar question to the CJEU.[38] It seeks to know whether Facebook can rely on the Article 6(1)(b) contractual necessity provision in place of Article 6(1)(a) consent to process personal data for the provision of personalised advertising. Perhaps more significantly, the Austrian court also invited the CJEU to clarify how the data minimisation and purpose limitation principles as provided by the GDPR should apply in the context of personalised online advertising, in particular when it comes to sensitive data. The Court's findings in this case will have important implications for all forms of big data processing.

3. Domestic Enforcement of Data Protection Law

The FIDE questionnaire sought to identify potential divergences between States concerning the domestic enforcement, both public and private, of the GDPR. There are now several relevant references pending before the CJEU.

On the relationship between NSAs and Courts, the CJEU is asked to clarify the meaning of the notion of "acting within a judicial capacity". According to Article 55(3) NSAs are not competent to supervise processing operations of courts acting in their judicial capacity. The case concerns the practice in the Dutch Council of State to allow journalists on the day of a hearing to read, on the spot, certain procedural documents from the file ahead of the hearing. When a person involved in a case before the Council of State lodged a complaint about this practice with the Dutch NSA, the NSA refused to accept the complaint, based on its lack of competence to supervise courts. In a thought-provoking opinion, Advocate General Bobek suggested that the CJEU employ a broad interpretation of the concept of "judicial capacity", going beyond mere judicial decision-making in an individual case, as was argued by the applicant in the national case.[39] Specifically, any activities that may indirectly impact upon their judicial independence must be covered and courts should, by default, be considered to be acting in this capacity unless it can be shown that a particular activity is of an adminstrative nature.[40]

In a reference from a Hungarian regional court, the CJEU is asked to provide guidance on the relationship between the rights found in Articles 77(1) and 79(1) GDPR (respectively the right to lodge a complaint with a supervisory authority and the right to an effective judical remedy against a controller or processor).[41] In particular, the referring court queries whether NSAs have priority competence over courts who have been asked, based on Article 79(1) GDPR, to determine the existence of an infringement and what impact Article 47 EU Charter has on the interpretation of this relationship. It also asks the CJEU whether the independence of NSAs enables them to adopt a different interpretation of the GDPR to a court in respect of the same alleged infringement.

The issue of what constitutes "harm" raised in the questionnaire for national rapporteurs features in two pending references. An Austrian court queries whether infringement of GDPR is in itself sufficient for an award of damages pursuant to Article 82 GDPR or whether the data subject must also have suffered harm. It also queries whether EU law requirements, beyond equivalence and effectiveness, influence the assessment of compensation and whether it is compatible with EU law to require something beyond upset for an award of non-material damages.[42] The Bulgarian Supreme

[38] Case C-446/21, *Maximilian Schrems v Facebook Ireland Ltd*.
[39] Opinion of Advocate General in Case C-245/20 *X and Z v Autoriteit Persoonsgegevens*, para 100.
[40] Ibid.
[41] Case C-132/21 *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság*.

[42] Case C-300/21 *UI v Österreichische Post AG*.

Administrative Court queries whether the worries, fears, and anxieties (without further data misuse or harm) experienced by data subjects because of a breach of confidentiality constitute non-material harm entitling them to compensation.[43]

The Austrian Supreme Court of Justice has asked the Court whether Article 80(2) GDPR allows competitors, associations, entities and Chambers to sue the data controller for an alleged breach of the GDPR.[44] These entities are entitled to initiate proceedings pursuant to national consumer law. Article 80(2) enables "any body, organisation or association *referred to in paragraph 1"* to complain to an NSA or to go before a Court without the mandate of a data subject. Article 80(1) GDPR refers to organisations that are:

> a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data

It seems unlikely that competitors will fit this description, although their private action may ultimately benefit data subjects by vindicating their rights. Furthermore, it is doubtful whether associations which had standing before the GDPR entered into force, will meet the requirements of Article 80(1) of the GDPR. The case also raises questions about the interaction with the recently adopted Directive on collective redress (Directive 2020/1828).

The German Facebook case (referred to above) is likely to be a pivotal one when it comes to delineating the boundaries between NSAs and other actors, specifically other regulatory authorities. From a substantive perspective, these proceedings have already attracted a lot of attention given that the German Competition Authority grounded its initial findings in the GDPR. The referring court queries whether it is possible for a national competition authority to determine that there has been a breach of the GDPR. The concern has been expressed that such a finding would undermine the GDPR's one-stop-shop system. The national referring court alludes to this through its observation that the Irish Data Protection Commissioner, the lead authority in the EU for Facebook, was investigating the same alleged GDPR breach. This judgement will therefore confirm whether the NSAs have exclusive competence as administrative authorities, to interpret and enforce the GDPR. The future consequences of the Court's findings may also be relevant to the various regulatory initiatives now in the legislative pipelines (see below).

These questions will provide welcome guidance on the relationship between public and private enforcement and how to deal with concurrent regulatory and legal proceedings under the GDPR. Given the numerous legislative proposals pending at EU level, such guidance may help to preempt contentious institutional issues.

Finally, it is necessary to mention that the Court has already had the opportunity to provide some further guidance on the more European dimension of data protection enforcement: the one-stop-shop procedure. In *Facebook Belgium*[45] the Court was asked to consider whether an NSA that was not the lead NSA under the GDPR can initiate legal proceedings to bring to an end an infringment concerning cross-border data processing. In this judgement, the Court confirmed that the general rule is that the lead supervisory authority is competent to adopt an infringement decision with the competence of

[43] Case C-340/21 *Natsionalna agentsia za prihodite*.
[44] Case C-319/20 *Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände*.

[45] Case C-645/19, *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit* EU:C:2021:483.

other NSAs to adopt such a decision being the exception. The Court emphasised, nevertheless, that the lead supervisory authority must "exercise such competence within a framework of close cooperation with the other supervisory authorities".[46] Moreover, the Court held that where an NSA exercises its power to bring infringements to the attention of judicial authorities this would equally undermine the objective and effectiveness of the 'one-stop shop' mechanism.[47]

4. Data Processing for National Security Purposes

The CJEU added a new chapter to the longstanding debate on the lawfulness of national measures that require telecom operators to retain or otherwise process traffic and location data of their costumers in order for that data to be avaiable for law enforcement or national security purposes. After the seminal *Tele2 Sverige* ruling, several Member States argued that the CJEU would not be competent to assess such measures if the objective was to safeguard national security. As described in the institutional report, this reasoning was based on the statement in Article 4(2) TEU that national security remains the sole responsibility of the Member States, as well as on the clause in the applicable data protection rules (the ePrivacy Directive) that excluded activities for the purpose of national security from its scope.[48]

In October 2020, the CJEU issued two rulings in cases stemming from Belgian, French and UK Courts. Following its logic in the *Tele2 Sverige* ruling, in which the Court discussed the exclusion of law enforcement activities from the scope of the ePrivacy Directive, but also took into account that the same ground appeared in the provision which allowed derogations from certain rights and obligations in the ePrivacy Directive, the CJEU concluded that the national measures at issue fell within the scope of the CJEU's jurisdiction.

The CJEU underlined that the activities that were excluded from the scope of the ePrivacy Directive concerned activities of the state. Since the national measures at issue involved the processing by telecom providers of traffic and location data, such activities could not be covered by the exclusion.[49] Only where Member States directly implement measures without imposing processing obligations on providers the protection of the data of the persons concerned is not covered by the ePrivacy Directive.[50]

In its subsequent analysis the CJEU set out the hierarchy amongst the different objectives that are sought by the measures at issue, placing the objective of safeguarding national security at the top, considering that is goes beyond the other objectives listed in the ePrivacy Directive, including the combating of (serious) crime and safeguarding public security.[51] The CJEU also provided a description of what national security entails:

> That responsibility [i.e. national security] corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.[52]

[46] Ibid, para 63.
[47] Ibid, para 65.
[48] Institutional Report at p.99-101.
[49] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* para 39 and Case C-511/18 *La Quadrature du Net and Others v Premier ministre and Others* (LQdN) para 96.
[50] Privacy International para 48 and LQdN para 103.
[51] LQdN para 136.
[52] Ibid para 135.

Because of the higher importance of the objective of safeguarding national security, according to the CJEU, generalised and indiscriminate retention is not per se excluded for that objective. This is an important consideration since the CJEU, in the *Tele2 Sverige* ruling, had concluded that such retention was excluded when the objective is fighting serious crimes. The CJEU formulated the circumstances in which such a generalised and indiscriminate retetention measure could be lawful for safeguarding national security, emphasising that it should be temporary and put in place because of a serious threat to national security which is shown to be genuine and present or foreseeable.[53]

Also on the national security of third states, the case law of the CJEU developed further. In the anticipated *Schrems II* ruling[54], the CJEU assessed whether the European Commission, in its EU-U.S. Privacy Shield adequacy decision, drew the right conclusion as to the essentially equivalent level of protection offered by the United States when US security agencies have access to personal data transferred on the basis of the EU-U.S. Privacy Shield. The EU-U.S. Privacy Shield was adopted after the CJEU in the first *Schrems* ruling invalidated the so-called Safe Harbor adequacy decision, which did not contain any analysis of the US legal framework on national security. Despite the elaborate description of the US framework in the EU-U.S. Privacy Shield decision, the consideration of new developments in the US legal framework and the introduction of a dedicated ombudsperson-mechanism, the CJEU again concluded that the safeguards offered were insufficient in the light of Article 7, 8 and 47 of the EU Charter of Fundamental Rights.

In the same *Schrems II* ruling, the CJEU left intact a decision of the European Commission which lays down Standard Contractual Clauses (SCCs), These SCCs can be relied upon by persons transferring personal data from the EU to third countries in a contract with the recipient of the data in the third country. The SCCs allow to provide for appropriate safeguards within the meaning of Article 46 of the GDPR. However, this is not automatic. The CJEU underlined that use of these appropriate safeguards should ensure that the personal data transferred are afforded a level of protection essentially equivalent to that which is guaranteed within the EU.[55] This requires the person relying on the SCCs to also take into consideration the relevant aspects of the legal system of the third country as regards any access by the public authorities to the personal data.[56]

II. Data Protection in its Broader Context

5. Data protection in a global health crisis

From the early days of the the COVID-19 pandemic, governments and public health authorities worldwide turned to data processing and technological solutions to mitigate its considerable impacts on society. Governmental and private sector responses[57] focussed on personal data collection and sharing in the context of epidemiological surveillance, contract tracing technologies including mobile apps, possibilities to use and re-use sensitive health data for scientific research and public health purposes, and the like. This resulted in considerable pressure on privacy and data protection, underlining the need for pragmatic approaches that would allow the reconciliation of the protection of individuals' fundamental rights with the need to combat a public health emergency.

[53] Ibid para 137.
[54] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (*Schrems II*) EU:C:2020:559.
[55] *Schrems II* para 96.
[56] Ibid, para 104.
[57] https://ec.europa.eu/info/sites/default/files/recommendation_on_apps_for_contact_tracing_4.pdf

From a legal perspective, the challenges were compounded by the fact that the EU competence in the area of public health is very limited and a Treaty legal basis for harmonising approaches is often lacking. At the same time, data concerning health constitute so-called special category data (often referred to as "sensitive data") subject to a very strict regulatory regime[58]. As a consequence, most of the traditionally available legal grounds that allow for lawful processing of personal data were not available, and in most cases a recourse to EU or national law was necessary, often resulting in tensions with the need to respond quickly to a rapidly changing epidemiological situation.

Throughout 2020, the Commission has issued a Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. The eHealth Network[59] has published a common toolbox[60] on the use of mobile applications to support contact tracing in the EU's fight against COVID-19, as well as interoperability guidelines[61] for approved contact tracing mobile applications in the EU. The Commission has also provided Guidance on Apps supporting the fight against Covid19 pandemic in relation to data protection[62].

Against this background, both the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) emphasised from the outset the need for a pan-European approach in tackling the pandemic. Both bodies issued practical guidance in relation to the most pressing challenges of the pandemic, stressing that pandemic-related technologies requiring the processing of personal data must be temporary, have a defined and limited purpose, and comply with EU data protection law.[63] As the supervisory authority responsible for the monitoring of personal data processing by EU institutions, bodies, offices and agencies (EUIs), the EDPS issued guidance in order to support EUIs in their effort to adopt the necessary health and safety measures in the workplace in compliance with the applicable data protection rules.[64]

One of the most consequential initiatives adopted at EU level is the legal framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate).[65] An EU Digital

[58] Article 9 GDPR and Article 10 EUDPR.

[59] A voluntary network set up under article 14 of Directive 2011/24/EU, and providing a platform of Member States' competent authorities dealing with digital health

[60] https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf

[61]https://ec.europa.eu/health/sites/default/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

[62] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN

[63] See EDPB guidance on the use of location data and contact tracing applications: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en; and the EDPB guidance on the use of health data for the purpose of scientific research purposes: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

[64] See EDPS Orientations on body temperature checks: https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-edps-body-temperature-checks-eu_en; manual contact tracing: https://edps.europa.eu/system/files/2021-02/21-02-02_orientations_on_manual_contact_tracing_euis_en_0.pdf;, and reactions of EUIs as employers: https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-edps-reactions-eu-institutions_en .

[65] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (OJ L 211, 15.6.2021, p. 1) and Regulation (EU) 2021/954 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic (OJ L 211, 15.6.2021).

COVID Certificate is a proof (via a QR code in a digital and paper format) that a person has either been vaccinated against COVID-19, received a negative test result, or recovered from COVID-19, valid in all EU countries and supported by an IT infrastructure that allows for the validity of the certificate to be verified across all EU Member States, as well as in a number of third countries.[66] The regulations adopted at EU level cover the use of the EU Digital COVID Certificate to facilitate safe free movement inside the EU. However, Member States can also use the COVID-19 certificates for domestic purposes, such as access to events or venues.

Despite the rather obvious tension with the principle of purpose limitation[67], this possibility to re-use the certificate at national level for purposes not limited to the free movement of persons was not excluded by EU data protection authorities in the Joint Opinion 04/2021 issued by the EDPB and the EDPS in response to a consultation request pursuant to Article 42(2) EUDPR.[68] As a clear sign of a pragmatic approach under extraordinary circumstances, the NSAs chose instead to focus on conditions for such possible further uses at national level which always require a clear and comprehensive legal framework to be adopted in order to ensure, among other things, that it should not legally or factually lead to discrimination based on having been (or not been) vaccinated or having recovered from COVID-19. The EDPB and the EDPS considered that such a legal basis in Member State law should at the very least include specific provisions clearly identifying the scope and extent of the processing, the specific purpose involved, the categories of entities that can verify the certificate as well as the relevant safeguards to prevent abuse.

The extraordinary nature of the Regulation on the EU Digital COVID Certificate is clearly visible in the fact that it will apply for 12 months as from 1 July 2021 (although the Commission will have a possibility to propose to extend its duration if necessary, taking into account the evolution of the epidemiological situation on the pandemic, based on a report to be presented to the European Parliament). It will indeed be important to ensure that exceptional measures deployed in times of crisis remain limited in time, and not become part of the "new normal". Only then will it become clear whether the EU data protection rules withstood the test of the COVID-19 crisis.

6. The changing regulatory context in which GDPR applies

Those familiar with the GDPR will concede that it is a complex piece of EU legislation, with a correspondingly complicated relationship to national law. In some respects, the GDPR builds on national law (e.g. grounds for lawful processing in Article 6), or conversely allows or mandates national law to build on it and thus give effect to its provisions (e.g. the provisions on the organisation and functioning of the supervisory authorities). Other provisions of the GDPR allow or require national law to specify or further develop its rules in certain areas (e.g. specific data processing situations in Chapter IX) or even to depart from its provisions under certain conditions (see in particular Article 23 GDPR)[69].

But what seems even more challenging is to describe the relationship between the GDPR and other instruments of *EU law* which have a bearing on the processing of personal data.

---

[66] See https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#potential-use-of-certificates-for-access-to-facilities for more information.

[67] Article 5(1)(b) GDPR and Article 4(1)(b) EUDPR.

[68] Available at: https://edps.europa.eu/system/files/2021-04/21-03-31_edpb_edps_joint_opinion_digital_green_certificate_en_0.pdf

[69] For a detailed discussion, see the Opinion of the European Data Protection Supervisor of 7 March 2012 on the data protection reform package, available at: https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

Early examples of EU acts that led to lengthy discussions about how their provisions should be interpreted alongside the GDPR (or *reconciled* with it) include the PSD2 Directive[70], Directive (EU) 2019/1770 on digital content[71], or the Regulation on the free flow of non-personal data.[72] In some cases, guidance on the interaction or interplay between the legislative instruments in question and the GDPR has been provided by the EDPB[73] or by the European Commission.[74]

Since November 2020, the European Commission has presented several legislative proposals as part of the implementation of its European strategy for Data[75] which, when adopted, are bound to dramatically increase the complexity of the regulatory landscape. These include the proposals for a Data Governance Act[76] (DGA), the Digital Services Act[77] (DSA), the Digital Markets Act[78] (DMA), as well as the proposal for an Artificial Intelligence Act.[79]

While the proposals generally tend to state that they are *without prejudice* to the GDPR, this may not always be sufficient to resolve possible incompatibilities or conflicting interpretations, bringing the risk of introducing more legal uncertainty into an already young and dynamic area of regulation. For example, the notion of *data altruism* introduced in the proposal for the DGA[80] to cover situations where natural (or legal) persons would make data voluntarily available for reuse, without compensation, for "purposes of general interest, such as scientific research purposes or improving public services", appears to overlap, at least in part, with the concept of consent to the processing of personal data under the GDPR (which potentially covers purposes such as scientific research). At the same time, it is unclear whether it is intended to fully correspond to the GDPR understanding of consent, including the conditions for validity set out in Article 7 GDPR.[81]

---

[70] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

[71] See also Institutional Report Topic 2 at 3.1, p. 82.

[72] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59). See also the European Commission guidance on free flow of non-personal data which addresses the "interaction of free flow of non-personal data with the EU data protection rules": https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2749.

[73] See the European Data Protection Board (EDPB) Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0 adopted on 15 December 2020, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf.

[74] See the European Commission guidance on free flow of non-personal data which addresses the "interaction of free flow of non-personal data with the EU data protection rules": https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2749.

[75] Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[76] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.

[77] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

[78] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

[79] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.

[80] Data Governance Act (n 76 above) Article 2(10).

[81] See EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) Version 1.1, available at: https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf.

The question of the relationship of the future new law to the GDPR arises also in relation to the proposal for an AI Act which is based on Article 114 TFEU, but also on Article 16 TFEU "insofar as it contains specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purposes of law enforcement"[82]. In addition, one may wonder to what extent the proposed regulatory approach relying on existing product safety/market surveillance regulations and standardisation can be effective in safeguarding the fundamental right to privacy and data protection.[83]

Finally, the new proposals raise the question of effective enforcement of the rules, including the powers and responsibilities of the supervisory authorities for data protection. As the EDPB and the EDPS observe in their Joint Opinion 5/2021, most of the AI systems within the scope of the proposed AI Act will be based on the processing of personal data, or will process personal data, while the supervisory authorities for data protection will not necessarily be considered "competent authorities" under the AI Act.[84]

Finally, the new proposals each provide for a slightly different and often complex governance model, usually involving the Commission, various national competent authorities and an advisory committee, an expert group or another "Board" to be set up at EU level. Crucially, the involvement of supervisory authorities for data protection is not always guaranteed, and provisions for institutionalised and structured cooperation between relevant competent authorities is not explicitly provided. Such cooperation should ensure in particular that all relevant information can be exchanged with the relevant authorities - including NSAs - so they can fulfil their complementary role, while acting in accordance with their respective institutional mandate.[85]

[82] AI Act (n 79) Explanatory memorandum p. 6 and recital (2).

[83] For a discussion of this and other aspects, see EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) available at: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[84] Ibid., at 2.5 p. 13.

[85] See also EDPS Opinion 1/2021 on the Proposal for a Digital Services Act of 10 February 2021, available at: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf and EDPS Opinion 2/2021 on the Proposal for a Digital Markets Act, available at: https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.