FIDE XXIX Congress The Hague 2020

The New EU Data Protection Regime

Questionnaire Topic 2 - FIDE XXIX Congress, The Hague, 2020

Associate Prof. Orla Lynskey (London School of Economics)[1]

General Introduction

The new EU data protection package entered into force in May 2018, following a protracted legislative process. The package comprised a General Data Protection Regulation (Regulation 2016/679, GDPR) and a lesser-known Law Enforcement Directive (Directive 2016/680, LED). The GDPR, in particular, seeks to "Europeanise" data protection law and to render it more effective: by introducing a regulation rather than a directive, an attempt is made to minimise national divergence while significant new avenues for private redress and public enforcement are introduced. Although the responsibility for public enforcement of the framework lies primarily with national supervisory authorities (NSAs), the creation of a new European body with the power to issue authoritative opinions and, in specific cases, binding decisions has a centralising effect on data protection enforcement. The hope is that the changes brought about by the GDPR will ultimately enhance the effectiveness of the EU Charter rights to data protection and privacy. Yet, despite this shift towards a truly European legal framework for data protection, and unusually for a regulation, the GPDR leaves much responsibility to the national legislature, NSAs and courts.

This new regulatory framework raises substantive, procedural and institutional issues that will of interest and relevance to general EU lawyers and those specialising in other fields of substantive EU law.

Those with an interest in procedural and institutional matters will note that the GDPR sets out detailed provisions on remedies, liability and penalties. These provisions specify high administrative fines and provide for the possibility of criminal sanctions, as well as introducing provisions providing for representative actions by non-profit organisations. These detailed remedies, avenues for redress and sanctions will need to be accommodated within the national legal system in a way that is compatible with the general principle of national procedural autonomy. Moreover, the similarities between the enforcement possibilities afforded by the GDPR and those applicable to financial services in the EU (in particular, the power of an EU body to issue decisions binding on national regulators) will not go unnoticed.

From a substantive perspective, the application of the EU Charter rights to data protection and privacy has had a transformative effect on the fundamental rights landscape in Europe. How the EU Charter has impacted upon domestic legal systems in this area as well as the impact of the GDPR on other rights, such as freedom of expression, is therefore covered in this questionnaire. Furthermore, the CJEU has been pushing the boundaries of the Charter right to respect for privacy in the context of law enforcement. The relevance of this

[1] o.lynskey@lse.ac.uk

jurisprudence to domestic national security interests, and thus issues of sovereignty, remains contested.

Beyond these broader EU law questions, this questionnaire addresses issues that are specific to the EU data protection framework. Although necessarily drafted in a technical and legalistic manner, these issues are of fundamental societal interest. For example, following the Facebook-Cambridge Analytica scandal, there has been renewed public interest and debate regarding the handling and harvesting of our data by technology giants and the bargain we have entered into with these actors (access to 'free' services in exchange for this personal data processing, addressed in question 5). Similarly, whether individuals should have a right to delete their data from the de facto public record (for instance, a search engine service like Google) when there is a countervailing public interest in this information is hotly contested and addressed in question eight.

The ambition of this questionnaire is to gauge how this new legal framework for data protection has been received by all relevant actors at national level (most notably, Courts; national Parliaments; national supervisory authorities; and civil society). This national data will then be used to inform the discussion of both the specific data protection questions and the general EU law issues that the new legal framework entails.

This being so, this questionnaire is structured around four key areas of inquiry:

A. Setting the Scene
B. The Reception of Substantive GDPR Provisions in the National Legal Order
C. Domestic Enforcement of Data Protection Law
D. Data Processing for National Security Purposes

A. Setting the Scene

The GDPR is unusual in so far as it is a Regulation that leaves significant scope for the national legislature to avail of the flexibilities incorporated in many provisions.

Question 1: *Please identify and describe the main national legal instruments that have been introduced to implement the GDPR. In particular, outline how these instruments avail of the most notable flexibilities incorporated in the GDPR (in, for example, Article 6(1)(c); Article 23 and 86-90 GDPR) and what oversight role the national supervisory authority (NSA) exercises in relation to these instruments.*

The EU Charter is unique amongst international human rights instruments in so far as it incorporates distinct provisions to protect the right to respect for private life and the right to data protection (Articles 7 and 8 EU Charter).

Question 2: *Does your national legal order differentiate between these rights? Has the EU Charter right to data protection influenced the interpretation of national law?*

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

While EDPB guidelines should minimise divergence between Member States on the interpretation of the GDPR's substantive provisions, even in this situation the possibility remains that the acceptance of the EDPB's findings remain contested at national level (for instance, by the judiciary; by other relevant regulators; by academics; or, by civil society and the media). It is for this reason that the following questions are asked.

GDPR Responsibilities

Many of the safeguards, or 'principles', relating to data processing remain unchanged from the 1995 Data Protection Directive. Yet, the meaning and practical impact of critical principles remains underdeveloped with limited guidance, to date, from the Court of Justice of the EU (CJEU).

Question 3: *How have data controllers interpreted and applied the principles of 'fair' processing; purpose limitation and 'data minimisation'? Has the NSA applied these principles and have they been interpreted by domestic courts?*

The Article 29 Working Party provided an Opinion on the use of 'legitimate interests' as a legal basis for data processing and, more recently guidelines on the concept of consent (endorsed by the EDPB).

Question 4: *How have these legal bases – 'consent' and 'legitimate interests' – arguably the most significant yet opaque in the digital environment – been interpreted by national courts?*

Most digital services and content offered to Internet users are offered for free-at-the-point-of- access to end-users. This service or content is then subsidised through the provision of online behavioural advertising tailored to the user based on a profile generated through the processing of their personal data. In this way, personal data becomes the indirect counter-performance or 'payment' for the provision of the 'free' digital content or service. Article 7(4) GDPR stipulates that, in situations where consent is used to justify personal data processing, when assessing whether consent is freely given, utmost account should be taken of whether the performance of a contract is made conditional on consent to the processing of unnecessary data. Similarly, Article 6(1)(b) provides that processing is lawful when 'it is *necessary* for the performance of a contract to which the data subject is party' (emphasis added).

Question 5: *Has there been debate or decision at national level regarding the validity of personal data as 'counter-performance' for the provision of digital content?*

GDPR Rights

The GDPR seeks to render existing rights (such as the right of access to data by the data subjects) more effective by specifying their meaning while introducing one 'brand new right', a right to data portability.

Question 6: *Article 22 provides for a right not to be subject to automated decision-making, including profiling. Article 22(2)(b) allows Member States to introduce legislative measures to ensure this right does not apply in certain situations. Have such legislative measures been introduced and, if so, what measures to safeguard the rights, freedoms and legitimate interests of data subjects do they incorporate?*

Question 7: *How has the right to erasure (Article 17), or its Data Protection Directive predecessor (Directive 95/46 EC, Article 12) been applied at national level by search engines, the NSA or Courts?*

Question 8: *The GDPR allows Member States to legislate to reconcile the right to data protection with freedom of expression (Article 85). Has your state introduced a law pursuant to Article 85(2) GDPR and, if so, how has this been interpreted and applied to date?*

C. Domestic Enforcement of Data Protection Law

The GDPR revolutionises the enforcement of data protection in Europe. On the one hand, it introduces a new EU body, the European Data Protection Board (EDPB) with the power to adopt authoritative opinions and, ultimately, even binding decisions on any matter of general application or producing effects in more than one Member State.[2] On the other hand, it introduces an array of new remedies and penalties, including significant administrative sanctions and the possibility for collective redress. The interaction between these new provisions and existing national procedural rules is likely to be complicated. It is against this backdrop that the following questions are asked.

NSAs are the guardians of the GDPR: they are tasked with the role of monitoring its application and contributing to the consistency of such application.

Question 9: *Identify the relevant public authority (or authorities) in your Member State. Outline its composition; the appointment process for members and staff; any additional power or duties the NSA is entrusted with under national law; and, provide relevant details regarding its 'enforcement record' under the GDPR.*

The GDPR provides individuals with a right to lodge a complaint before a supervisory authority and states that the supervisory authority shall inform the complainant on the progress and outcome of that complaint. Some commentators have advocated that supervisory authorities should adopt a 'selective to be effective' approach to complaints by triaging them to focus resources on the most significant (for instance, in terms of scale or legal precedent).

[2] This results from a combined reading of Article 64(2) and Article 65(1)(c) GDPR.

Question 10: *What strategy for complaint-handling is taken by your NSA and what, if any, constraints does domestic law place on such a strategy?*

The GDPR provides Member States with new mechanisms to sanction data protection infringements, including the power to impose corrective measures (Article 58(2)), enhanced administrative fines (Article 83) and the possibility to impose 'other penalties' (Article 84 GDPR).

Question 11: *How have these sanctions been applied by your NSA, and what additional sanctions have been adopted at national level in addition to those explicitly provided for by the GDPR?*

The GDPR provides that data subjects should be compensated for damages suffered for tangible and intangible harm (Article 82).

Question 12: *Has your legal system historically awarded damages for intangible harm (in this area or others)? If so, how are such damages calculated?*

Data processing operations in the online environment in particular can be characterised by information and power asymmetries between data controllers and data subjects. The GPDR seeks to mitigate these asymmetries by providing for the possibility of representative actions pursuant to Article 80 GDPR.

Question 13: *Has your Member State introduced legislative measures to facilitate such representative actions? What role have NGO's played in data protection enforcement in your State and are there any alternative movements emerging at national level (such as personal data cooperatives or unions) to combat such asymmetries?*

As personal data has both an economic and a dignitary value there is an increasing trend for regulators beyond NSAs to intervene in data processing related complaints (for instance, competition authorities and consumer protection authorities). Moreover, in some states new regulatory bodies for the Internet and/or Artificial Intelligence are proposed.

Question 14: *Have these trends been visible in your Member State? In particular, has the NSA cooperated with other regulators or an ombudsperson formally or informally?*

D. Data Processing for National Security Purposes

Both the GDPR and the Law Enforcement Directive exclude from their scope of application personal data processing for 'national security' purposes. The Law Enforcement Directive seeks, for the first time, to regulate the domestic data processing operations of law enforcement authorities. The dividing line between law enforcement activities, within the Directive's scope, and national security activities, outside its scope, may therefore give rise to contestation at national level.

Question 15: *Is 'national security' defined in your domestic law or administrative practice? Have national authorities accepted the application of the EU Charter to data retention for national security purposes (following from the* Tele 2 *and* Watson *judgments)?*