Research Note no. 22
March 2017

CREOGN Research Note

Gendarmerie Nationale Officers College Research Center

The General Data Protection Regulation: towards an EU "bill of rights" on digital identification?

Published in the Official Journal of the European Union on May 4, 2016, the General Data Protection Regulation (EU) 2016/679 of the European Parliament and Council dated April 27, 2016 "*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*" has come into force as of May 25, 2016. A parallel can be drawn between this new Regulation and the eighth centenary of Magna Carta[1],which already consecrated as an essential principle the safeguard of personal rights and freedoms. As of May 25, 2018, the Regulation will create such enforceable rights as it becomes fully opposable in its entirety before all jurisdictions of the 28 Member States of the European Union. During the transitory period, no Member State will be allowed to legislate in contradiction to its provisions. Ultimately, this legal text completes the unification of the 28 different legislations on personal data protection, absorbing in particular France's law no. 78-17 dated January 6, 1978[2]. Henceforward, the protection of personal data will belong to a single legal corpus, directly transferable into the national legislations of EU Member States.

Our commentaries in this research note will highlight one of the major effects of this Regulation, namely the creation of a common definition of what constitutes personal data. This definition - a frequent source of controversy in both doctrine and case law - has long been fluctuating. Regarding the general philosophy guiding its authors, the EU Regulation is intended – as stated by the European Commission – as an appropriate political and judicial stance designed to provide better answers to the "*new challenges*" arising from "*rapid technological developments and globalization*"[3].

The application and interpretation of some of its provisions are bound to affect the bases of democratic societies in Europe over the next decade. Two related EU Directives published at the same time as this Regulation will also have an indirect impact on the concrete implementation of law and order policies within Member States. The present note will limit its scrutiny to the essential points of the Regulation, which – in themselves and in this perspective – lay the foundations for an EU-wide charter or "digital bill of rights" protecting citizens and their freedoms from current or potential excesses in this new and open field.

The General Data Protection Regulation (GDPR) sets forth a common definition for both personal and sensitive data which *de facto* creates a protective shell for all citizens (see section I below). Within this shell, citizens enjoy stronger rights (section II) allowing them better means of remedy in the event of any act likely to infringe on their fundamental rights in the field of digital identification. Finally, the introduction of administrative sanctions and the appointment of data protection delegates within organizations as part of an overall framework of data governance based on the principles of *accountability*[4] and *compliance*[5] should make the new Regulation truly efficient (section III).

1 "*The Magna Carta Libertarum or Great Charter of Liberties (1215) is the document imposed by English barons on their king, John Lackland, to force him to acknowledge and protect the freedoms and privileges of the nobility*". cf. *Dictionnaire de la science politique et des institutions politiques*, Armand Colin, 8th edition, 2015, p.176.

2 For an account of this process, see the information report of the National Assembly (AN no. 4544 dated February 22, 2017), compiled by French MPs Anne-Yvonne Le Dain and Philippe Gosselin. http://www.assemblee-nationale.fr/14/pdf/rap-info/i4544.pdf

3 OJEU - 04052016- L119/2 – Preamble, (6).

4 Defined as *"an English legal term referring to the obligation of accounting for one's actions and of taking corresponding responsibility". Cf. Lexique de science politique, vie et institutions politiques,* Dalloz, 3rd edition, p. 2.

5 Another English word which – for companies and other organizations - might be defined as "*conformity to the values and ethical standards formally defined by their managers—together with all necessary processes to ensure such conformity*". Lack of conformity may result in judicial or administrative sanctions, financial penalties or damage to the image or reputation of the organization.

I) A single definition of what constitutes personal data within the EU

The EU Regulation does not apply to fields connected with the – broadly understood - sovereignty of Member States, including their own national security[6]. As for France, its law dated July 24, 2015 governing intelligence gathering thus remains immune by its very nature. Neither does the GPDR interfere with the various cultural traditions and religious beliefs of EU nations: personal data connected with deceased persons do not come within its remit[7]. Overall, the GPDR concentrates rather on protecting individuals in their social, professional and economic activities. However, the Regulation is carefully designed not to hamper innovation based on the processing of personal data—provided such innovative developments remain oriented towards the common good of citizens.

a) Harmonized wording

The consolidated wording used for the definition of what constitutes personal and sensitive data will now compel Independent Supervisory Authorities (ISAs)[8] and jurisdictions to refer their decisions to Article 4 of the Regulation, which defines such data as follows: "*Any information any information relating to an identified or identifiable natural person (...); **an identifiable natural person** is one who can be identified, directly or indirectly, in particular **by reference to an identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".* The Regulation is therefore destined to apply to the activities of any organization – including subcontractors - processing personal data belonging to citizens of the European Union[9] as part of its offers of goods and services. More specific definitions have also been provided in the articles of the Regulation concerning the notion of sensitive data in the fields of genetics, biometrics and health[10]. Furthermore and regarding the legal capacity of minors to give consent to the processing of their personal data, a wide margin of interpretation is granted to Member States. Article 8 of the Regulation limits the possible age of consent between the ages of 13 and 16[11].

b) Balancing private interests with public interest

Drafters of the Regulation were keen to strike a delicate balance, insisting on the respect of fundamental rights while not hampering necessary exchanges of personal data flows. This balance is intended to create an anchorage point of stability and trust within democratic societies in order to prevent the undermining of their foundations. Section (4) in the preamble stipulates that: "*The right to the protection of personal data is **not an absolute right**; it must be considered in relation to its function in society and be balanced against other fundamental rights, **in accordance with the principle of proportionality**".* Article 9-2 defines three grounds for exception, namely compliance with a legal obligation, reasons of substantial public interest and the legitimate exercise of a public authority. For each of those three cases, the overall prohibition of disclosure set out by Article 9-1 does not apply[12].

---

6 Two EU Directives were published on the same day as the Regulation: Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data; Directive 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. For the latter, see CREOGN Research Note no. 19. Available at: http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Fichier-PNR-surveillance-electronique-de-masse-ou-nouveauparadigme-de-la-securite

7 Cf. OJEU, 04/05/2016 – L119/5 – Preamble, (27).

8 In France, this authority will be the "Commission nationale informatique et liberté" (National Commission on Computer Technology and Freedom, aka CNIL).

9 "European Union" is used here to refer to all Member States of the European Economic Area, i.e. the 28 Members States of the EU, plus Iceland, Liechtenstein and Norway.

10 Cf . Articles 4-13,14 and 15 of the GPDR, p. L.119/34.

11 For French positive law on the processing of personal data belonging to minors, cf. Law no. 2016-331 dated October 7, 2016, Articles 56 and 63. Such provisions were originally set out in Articles 58 and 40 of Law no. 78-17 dated January 6, 1978.

12 Cf. Article 9-1: "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*".

II) Stronger rights and monitoring--with deterrent administrative sanctions

The GPDR grants all persons a capacity to act against any organization - or subcontractor thereof - in control of an automated data processing system (ADPS) failing to ask for their free and informed consent prior to the registration of personal and sensitive data. Within this framework, the ISA plays a key role in terms of outside monitoring and handing down of administrative sanctions. Moreover, internal monitoring is also ensured by the Regulation, which mandates for all organizations – depending on the number of employees and/or the nature of activities – the appointment of a *Data Protection Officer (DPO)*[13] with specific powers. All these new measures are bound to contribute to the creation of new mode of data governance.

a) New rights for a new field

On a par with fundamental legal texts such as Magna Carta having established a certain number of rights intended to oppose arbitrary power, the GPDR is clearly designed to grant citizens legal means to thwart the excesses of our modern-day "information societies". At the heart of its purview lies the notion of consent, which the Regulation defines as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"[14]. Such a definition of consent lays the burden of accountability on the organizations in control of data processing.

Consent is also strengthened by the granting of new prerogatives to Internet users, aimed at ensuring compliance with adequate data governance on the part of ADPS controllers, i.e. based on principles of transparency and traceability. This "good governance" package includes a whole set of rights listed in a specific chapter[15]. Two among them have attracted special notice among law specialists: the right to erasure (or "right to be forgotten") and the limitations granted on profiling. Article 17 of the Regulation consecrates the right to deletion of data already acknowledged by the *Google Spain* decision of the European Court of Justice (CJEU)[16]. Subject to any of the six motives set out by Article 17, "*the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue dela*y". Likewise, provisions regarding automated individual decisions – generally associated with the notion of "profiling"[17] – will definitely impact future law theory in discerning what is freedom of choice. Indeed, highly sophisticated predictive algorithms coupled with artificial intelligence are bound to increase the capacity of systems to make automated individual decisions—with a major risk of manifest errors of appreciation and further non-accountability. In order to prevent those two problems, Article 22 grants the data subject "*the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*". However, this right is not understood as general and absolute and a number of exceptions – though strictly limited - are also provided. Finally, the recommended policies of transparency and trust intended to reassure citizens within the framework of the "new economy" are translated in Articles 33 et 34 which compel organizations to report any violation of personal data protection rights—both to the person or persons concerned and to the competent ISA.

b) Data regulation measures combining *hard law* with *soft law"*[18]

The new Regulation has learned from the inadequacy of the very limited sanctions mandated by EU Directive 95/46/EC dated October, 1995. Indeed, a number of commentators have only recently underlined how much – for instance – fines in the amount of €100,000 ordered by France's CNIL against Google Inc.[19] did not reflect

13 In France, DPOs will replace the former CILs ("Correspondants informatique et libertés")--with wider prerogatives. For concrete applications of the new Regulation, cf. www.cnil.fr/fr/consultation-reglement-europeen/dpo

14 OJEU - 04052016- L119/34, Article 4-11.

15 Cf. Chapter III : *Rights of the data subject,* OJEU, 04/05/2016, L.119/39.

16 Decision dated May 13, 2014. Available with the reference: ECLI:EU:C:2014:317.

17 Article 4-4 defines profiling as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

18 "Soft law" may be defined as follows: *"an English legal phrase referring to non-compulsory rules or provisions, i.e. without any judicial sanction attached to them."*

19 Deliberation no. 2016-054 dated March 10, 2016, taken in restricted formation and ordering a pecuniary sanction against the

the "*effective, proportionate and dissuasive*" character of sanctions now intended by the Regulation. From now on, ISAs will be empowered to inflict sanctions in the amount of tens or even twenties of millions of euros—equal to 2-4% of a corporation's yearly global turnover. However, the Regulation leaves to Member States the initiative of sanctions for other violations beyond those specifically referred to in its articles. Such *hard law* provisions are meant to bolster the legitimacy and effectiveness of the GDPR in the eyes of the big four Internet giants or "GAFA". Deterrence is also provided in the upstream context to detect intentional or unintentional infringements on the part of any organization or its subcontractors. The Regulation thus mandates the appointment of a DPO within public administrations and authorities (except for jurisdictions), as well as within private companies whose core activities are connected with large-scale data processing. Once appointed, the DPO "*does not receive any instructions regarding the exercise of [his/her] tasks*"[20]. He/she "*shall not be dismissed or penalized by the controller or the processor for performing his tasks*". DPOs are also empowered to monitor the conformity of the record of processing activities (Article 30), a real certificate of long-term traceability for all personal data flows. The second aspect of data protection is built around *soft law*, i.e. certification procedures designed to encourage the drafting of Codes of Conduct (Article 40) for all segments of data processing. Replacing the prior declaration already required for any ADPS, a new declaration of conformity with GDPR provisions is now imposed; organizations concerned will be responsible for informing their clients and partners of their corresponding status in accordance with the various recommended levels of certification for their data processing activities. With the aim of achieving the harmonization of the different certification standards currently applicable across the EU, the Regulation mentions the possibility of using common standards leading to the award of "*data protection seals*". The "e-reputation" of corporations and their governance in the field of personal data protection in particular will therefore depend on the award of such high-level certificates and their compliance with the provisions of their Codes of Conduct. This new approach to the regulation of personal data protection follows the recent trends in corporate standardization procedures driven – most prominently – by Northern American insistence on the value of *compliance*[21].

Conclusion

In the long run, the GDPR may prove – in many ways - to be one of the legal texts that give its full meaning to the EU project. Already possessing the scope of a future "bill of rights" and assuming an extensive territorial area of jurisdiction, this Regulation ambitions to exert influence over the GAFA giants and – subsequently – over the Northern American understanding of personal data protection. In her report to the Council of Europe[22], law philosopher Antoinette Rouvroy recently underlined the opposition between the American "law and economics" approach[23] and the European approach which differentiates data "*in accordance with the amount of power they confer on those controlling them and with the aim of trying to prevent massive informational inequalities of status between controllers and natural persons*". It now remains incumbent on the CJEU to give interpretation and reveal all potential consequences of this legal text. Even Machiavelli sometimes discovers that - as the French philosopher Claude Lefort once wrote - "*law within free cities is not always a creation of cold reason but rather the result of confrontation between two unlimited aspirations—that of the Powerful to own always more and that of the common people not to be oppressed. Law is therefore never given once and for all; it remains open to the conflicts that must always lead to its reform*"[24].

Google Inc. company. Cf. https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946

20 This acronym is used to refer collectively to Google, Apple, Facebook and Amazon.

21 "*Contrary to French "conformité" - which refers to a state of correspondence with a given standard – the English word "compliance" also refers to the process of standardization itself and thereby acquires a programmatic value for the behavior of corporations*" (Alain SUPIOT, *La Gouvernance par les nombres, Cours au Collège de France (2012-2014),* Fayard, Coll. Poids et mesure du monde, Paris, 2015, p.404. See also: www.cercledelacompliance.com/app/download/5783911672/Retranscription+ConfC3%A9rence+Cercle+De+la+Compliance+26012012.pdf

22 Report entitled "Of data and mankind. Law and fundamental freedoms in a world of mass data", p.7. Available at: http://docplayer.fr/13907024-Des-donnees-et-des-hommes-droits-et-libertes-fondamentaux-dans-un-monde-de-donnees-massives-antoinetterouvroy.html

23 This approach may be described as follows: "[an approach that] *in the allocation of resources (data being such), favors those most likely to create value out of their use. In this perspective, [it also favors] the organization of a data market in which personal data is considered as commercial goods (…) therefore allowing individuals to negotiate supply of "their" data against financial payment or other advantages (…). Supporters of the "law and economics" approach claim this is necessary to foster growth and innovation in the digital economy."* ROUVROY report (see previous footnote).

24 Quoted by SUPIOT, Op. cit., p.114.