ISSN 2704-8012

European Journal of Privacy Law & Technologies

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in Dicember 2019
www.ejplt.tatodpr.eu

HARD LAW AND SOFT LAW ON DATA PROTECTION: WHAT A DPO SHOULD KNOW TO BETTER PERFORM HIS OR HER TASKS

Maria Cristina Gaeta

Abstract

The paper aims to describe the sources of law needed to solve issues in data protection, with particular regard to DPO tasks. In order to elaborate this work, two preliminary steps have been carried out. The first one is focused on the critical analysis of the European and Italian law in the field of data protection. The sources of law include both hard law and soft law, with particular regard, for the second one, to the code of conduct. The second step is to define the relevant topics for DPOs, which are the matters that a DPO has to know to better perform his or her tasks in compliance with the GDPR, explaining the reasons underlying their selection.

Keyword: Data Protection Officer; GDPR; Code of conduct.

Summary: 1. Introduction. – 2. The sources of law on data protection with particular regard to the difference between code of conduct and common guidelines. – 3. An overview of the codes of conduct in Europe and in Italy. – 4. Main data protection topics for DPOs. – 5. Conclusions.

1. Introduction

This paper has been prepared as part of the deliverables for the EU-funded project entitled "Training Activities to Implement the Data Protection Reform" (TAtoDPR),[1] EU project aimed at training of data protection officers (DPOs), especially in specific sector which will be better illustrate below (*see* table 1), in their new duties under the General Data Protection Regulation (Regulation

[1] More precisely the TAtoDPR has ben co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020) under Grant Agreement n. 769191. For more information on the TAtoDPR project see: https://www.tatodpr.eu.

2016/679, well known as GDPR).[2] The project has been carried out under the guidance of University of Naples Suor Orsola Benincasa (coordinator of the project) and involved different European countries: besides Italy also the United Kingdom and Spain.[3]

As a matter of fact, GDPR is applicable since May 25th 2018,[4] replacing the Data Protection Directive (Directive 95/46/EC). The data protection regulation was adopted in response to the maximum extension of the processing of personal data and to the development of ever more pervasive technologies, strengthening the main EU data protection regime to the point to entail a real reform on data protection. GDPR brings many changes in terms of much greater harmonisation and cross-border enforcement cooperation between national Data Protection Authorities (DPAs) and the European Data Protection Supervisors (EDPS),[5] also thought the European Data Protection Board (EDPB), established

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1571686089135&from=IT. T

[3] Four Universities and an enterprise are involved in this European project, providing different perspectives and expertise:

Università degli Studi Suor Orsola Benincasa of Naples (UNISOB), is the Coordinator of the project TAtoDPR, with its outstanding tradition in the field of Law and New Technologies, and especially the Interdepartmental Research Centre 'Scienza Nuova' and its 'UTOPIA Lab' and the Research Centre of European Private Law (ReCEPL) both established at UNISOB, specifically dedicated to creating a bridge between social sciences and the realm of advanced scientific and technological development. UNISOB Legal team has already obtained several recognitions for its research activity in the field of data protection.

Universidad de Sevilla (USE) provides an expert team including lecturers and researchers in the fields of Civil Law, Privacy Law, Digital Law and Computer Engineering, providing diverse skills and know-how.

Loughborough University (LBORO), and more specifically the Loughborough Design School, is committed to the study of Cognitive and Behavioural aspects of data protection.

University of Derby (DER) contributes with a strong interest and competence in the fields of Law and Political Economy applied to the domain of Data Protection.

RE:Lab s.r.l. (REL) brings long-standing interest and experience in the field of HMI (Human-Machine Interface), including computers, smartphones and other devices, as well as in the relationship between individuals, technology and personal data.

[4] Even though, as a rule, the EU regulations come into force twenty days following the publication in the Official Journal of the European Union (OJ), under art 99 GDPR, the Regulation has been applicable after two years from the publication. It means that GDPR was effectively applied from May 25th 2018, but each single EU Member states needed different timeframes for the application of the GDPR in its legal system which depended on the type of regulatory modification to be put in place and this, sometimes, involved the application of the GDPR after the deadline set by art 99 GDPR.

[5] *See* the official website of the European Data Protection Supervisor (EDPS): https://edps.europa.eu. Currently, art 51 and ff. GDPR provides general DPAs' rules.

by the GDPR and which replaced WP29.[6] At the same time, data protection reform introduces new principles on data protection and introduces the new role of data protection officers (DPOs). The DPO also has the task of cooperating with the national or European data protection authorities and act as a contact point for the DPAs for matters related to the processing of personal data (article 39 GDPR).[7]

This paper attempt to briefly analyse the existing data protection regulation (hard law and soft law) in Europe and in Italy, as well as to identify what a DPO should know to better perform his or her tasks in compliance with the GDPR.

2. The sources of law on data protection with particular regard to the difference between codes of conduct and common guidelines

At the European level, as already explained, GDPR replaced the Data Protection Directive of 1995. The data protection reform was a consequence of the exponential increase in data processing also due to the development of ever more pervasive technologies.

The GDPR is a regulation and not a directive, so it is directly applicable in the legal systems of the EU Member States, without having to be transposed into national law, as is the case of the EU directives, included the Data Protection Directive, which bound the Member States only to the end to be achieved but not even to the means to achieve it. The choice for the regulation instead of the directive was well thought out by the European legislator since with the Data Protection Directive a different implementation had occurred at the national level, which resulted in a non-homogeneity of the protections. Contrariwise, the EU data protection regulation has strong harmonizing power. Indeed, although the GDPR has been applicable for just over a year, the national regulatory disciplines of the individual member states already seem more harmonized.

About the territorial scope of the legislation (articles 3-5, GDPR), reference is no longer made to the placement of the terminal into a Member State of the European Union but to the offer of services in EU countries. Therefore, the

[6] *See* the official website of the European Data Protection Board (EDPB): https://edpb.europa.eu. EDPB is regulated under art 68 and ff., GDPR.

[7] The DPO acts as a contact point in order to facilitate the access by the relevant DPA to the documents and information for the performance of the DPAs' tasks or power, respectively mentioned in artt. 57 and 58 GDPR. In particular, the DPO is bound by secrecy/confidentiality concerning the performance of his or her tasks, in accordance with EU or national law (Art 38, par. 5, GDPR). Nonetheless, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and advising DPAs (art. 39, par. 1, let e)).

GDPR is fully applied to companies located outside the European Union that offer services or products to data subjects in the territory of the European Union. Outside the European area, however, there is the general principle of the limitation of the circulation of personal data (purpose limitation and storage limitation) based on the conformity assessment of the guaranteed measures. Compliance with specific procedures and compliance with the data adequacy principle for the non-EU transfer of personal data is required or, failing this, is needed the explicit consent of the data subject or other particular conditions. [8]

Currently, the GDPR is the main hard law existing in Europe for the protection of personal data. However, there are many legislative initiatives to further implement data protection as, for example, the Proposal for an ePrivacy Regulation of 2017, which is a proposal for greater regulation of electronic communications within the European Union, to increase privacy for individuals and entities. More precisely, today the electronic communications are regulated under Directive 2002/58/EC on electronic communications (well known as ePrivacy Directive). Anyways, the directive seemed to not have a strong impact on data protection issues related to electronic communication, including automated processing issue. For this reason, the European Commission carried out an *ex post* Regulatory Fitness and Performance Programme ("REFIT evaluation") of the ePrivacy Directive and verified that the Directive has not guaranteed effective legal protection of privacy in the electronic communication, taking in to account the digital era in which we live. In particular, the REFIT evaluation shows how important technological and economic developments took place in the market since the last revision of the ePrivacy Directive in 2009. Consumers and businesses increasingly rely on new Internet-based services enabling inter-personal communications (e.g. Voice over IP, instant messaging and web-based e-mail services) which fall down the name of Over-The-Top communications services (OTTs). Generally, the OTTs are not subject to the current EU electronic communications framework which has not kept up with technological developments, resulting in a lack of protection of electronic communications. [9] At the end of the REFIT evaluation, indeed, on 2017 it has been published a Proposal for a

[8] The consent to the processing of personal data plays a central role in the GDPR, which specifies that the con sent must be freely given, specific, informed and unambiguous must consist of an express or explicit action signifies agreement to the processing of his or her personal data (art. 4, n.11, GDPR). Furthermore, the consent represents one of the lawful bases for the processing of personal data (Article 6, para 1, let a), GDPR) and of special categories of personal data (Article 9, para 2, let a), GDPR).

[9] Explanatory memorandum of Proposal for a Regulation of the European Parliament and of the Council, of 10 January 201,7 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM(2017) 10 final), 5.

Regulation on privacy and electronic communications (known as ePrivacy Regulation or ePR), which takes into account of the technological development of our society. [10]

In Italy, the transposition of the GDPR was operated by legislative decree no. 101/2018, [11] which led to significant changes to the Italian privacy code in force (legislative decree no. 196/2003) [12] that was compliant with the Data Protection Directive of 1995. The subsidiarity of the reformed Italian privacy code is evident already from the title of the code as amended, as well as, from the first articles, which show how the text contains provisions for the compliance of the national legislation to the provisions of the GDPR (art. 2 Italian privacy code). [13]

One of the main changes introduced by amendment decree is certainly that relating to minors. In particular, the age for expressing consent to data processing within the information society services is set at 14 years (article 2 *quinquies*, Italian privacy code), using the derogation provided by the GDPR which provides for a limit of 16 years reducible up to 13 (article 8, paragraph 2, GDPR). [14]

Regarding, the data protection in healthcare, the new Italian rule (art 2 *septies*, Italian privacy code) provides that the processing of personal data for the purpose of health protection is regulated under article 9 of the GDPR. The article establishes a general prohibition on the processing of special categories of personal data, except in specific hypotheses provided for by the same article. [15] The previous rule of the Italian privacy code authorised the processing of this particular type of data to the consent of the data subject and to the authorisation of the Italian DPA. The new legislation simplifies the situation by no longer providing for the authorisation of the Italian DPA. On the other hand, however, it requires enhanced data protection, introducing the possibility that the Italian

[10] Proposal for a Regulation of the European Parliament and of the Council, of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM(2017) 10 final).

[11] Provisions for the compliance of national legislation with GDPR, d.lgs. 10 August 2018 no. 101, OJ 205, available at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

[12] Italian Data protection code, d.lgs. 30 June 2003 n 196, OJ 174, available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678.

[13] Actually, the reformed Code is not only the compliance of national rules to European ones but also contains provisions that are not linked to the European regulation and states something more (eg. for the penalties).

[14] To in-depth the topic of data protection of minors in the digital environment, focusing on the issue of privacy digital consent given by a minor, *see* IA Caggiano, 'Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione' (1) 2018 Familia (online), 1 ff.

[15] See in particular art. 9, par.2, let. H) and i).

Data Protection Authority imposes specific guarantee measures for the treatment of health data (with a revised provision every two years).

Concerning the new privacy figures, in addition to the DPO, the modified Italian regulation, following the GDPR, allows the data controller or the data processor to designate natural persons for perform specific tasks and functions, related to the processing of personal data. These are not the internal data processors, who were required by the previous version of the Italian privacy code but are person in charge of processing (article 4, no. 10 and articles 29, GDPR).

An anther important news is that the Italian privacy code now provides the *Ente unico nazionale di accreditamento*, which is *Accredia*,[16] as the national accreditation body referred to in article 43, paragraph 1, letter b), GDPR. This statement does not affect the Italian DPA to directly assume the charge of such functions with reference to one or more categories of processing (article 2 *septiesdecies*, Italian privacy code).

Finally, the Italian privacy code provides not only administrative fines (art. 166, Italian privacy code) but also specific penalties for data breach (article 167, Italian privacy code), compared to the provisions of the GDPR that do not expressly provide penalties but only compensation for damages (article 82, GDPR) and administrative fines (articles 83 ff., GDPR). At the same time, however, GDPR, admits the possibility for Member States to establish other penalties (art. 84, GDPR), as well as other administrative fines for the infringements of national rules adopted within the limits of the GDPR (Recital 148) and Italy acted in this light[17].

Coming to soft law, codes of conduct are very important even though, at the moment, in the field of data protection codes of conduct are provided only at the national level. The codes of conduct are rules of conduct or uniform practices in general developed by various international, European or national bodies. They are non-binding provisions (i.e. the codes of conduct are soft law) even if the authority of the body they come from ensures that they are widely applied. The codes of conduct are tools of self-discipline that allow representatives and trade associations to define international, European or national rules to create uniformity within a specific sector (eg. data protection). This self-discipline rules should not be

[16] Accredia is a recognized association which operates on a non-profit basis, under the vigilance of the Italian Ministry of Economic Development. It is the sole national accreditation body appointed by the Italian government in compliance with the application of the GDPR, attesting «the competence, independence and impartiality of certification, inspection and verification bodies, as well as testing and calibration laboratories». For more information see the official website: https://www.accredia.it

[17] At the same time, the initial approach of compliance with the GDPR is rather soft, as expressly stated in art. 22 para 13, d.lgs. no. 101/2018, which foresees that for a period of 8 months the Italian DPA will have to take into account the fact that it is a new law, in the application of fines and penalties.

confused with the guidelines, which are a set of systematically developed information, based on continuously updated and valid knowledge, drawn up in order to make a desired behaviour appropriate and with a high-quality standard. Often, guidelines are produced by multidisciplinary groups and offer a broad definition of good practice. They are contained in documents brought to the attention of a group of interested parties and constitute a starting point for setting up shared behaviours in organizations of all kinds (both private and public) in the social, political, economic, corporate, medical and so on. Nevertheless, as the codes of conduct, the guidelines are soft law because they are not mandatory procedure.

Certainly, the codes of conduct play a very important role in the new data protection system. The GDPR, indeed, foresees the burden of proof, on the data controller (and to the data processor), that has to demonstrate to have implemented the adequate organizational and security measures for the protection of personal data (article 24, GDPR). The codes of conduct, therefore, can be used as evidence in this sense in avoiding high fines; however, the codes of conduct do not guarantee themselves the compliance with the GDPR.

3. An overview of the code of conduct in Europe and in Italy

In the European union, the codes of conduct are fundamental to avoid actions contrary to the GDPR by a specific category of data processor and data controller. This happens both because the codes of conduct contain the description of legal and ethical behaviours considered most appropriate in the reference sector and facilitate compliance with GDPR. In fact, the GDPR attaches great importance to codes of conduct and provides that Member States, Data Protection Authorities (DPAs), the European Data Protection Board (EDPB) and the Commission encourage the development of codes of conduct intended to contribute to the correct application of the GDPR, according to the specific needs of the different kind of the processing and that of micro, small and medium enterprises (art. 40, GDPR). On this point, moreover, the GDPR states that associations and other bodies representing the categories of data controllers or data processors may draw up codes of conduct, amend them or extend them, in order to specify the application of the provisions of the GDPR with particular regard to the topics expressly indicated in the article itself (among many others, for example, are mentioned the collection of personal data, the pseudonymisation, the exercise of the rights of the interested parties, as well as the notification of personal data breaches to DPAs.). [18] Code of conduct represents a way to apply the

[18] Aspects that could be regulated by codes of conduct are the following, as stated in art. 40,

accountability principle which consists in the obligation to assume responsible management that takes into account the risks connected to the activity carried out and that is suitable to guarantee the full compliance of the processing with the principles enshrined in the GDPR and national legislation. The result is the responsibility of the data controller and the data processor who are entrusted with the task of deciding autonomously the methods, the guarantees and the limits of the processing of personal data, also thanks to the adoption of codes of conduct. [19]

The associations and other bodies indicated in GDPR that intend to draw up a code of conduct, amend, or extend an existing one, have to submit the draft code to the DPA which is competent under Article 55 GDPR. The competent DPA expresses an opinion on the compliance with GDPR of the draft code, or the amendment, or the extension, and approves it, if it considers that it offers sufficiently adequate guarantees. If the DPA approves the code of conduct, it has to register the code and publishes it.

In the event that the draft code of conduct refers to the processing activities in different Member States, before approving the draft code, the amendment or the extension, the competent DPA submits it, through the so-called consistency mechanism (art. 63 GDPR), to the EDPB, which formulates an opinion on compliance with the GDPR of the draft code, its amendment or its extension. In the case in which codes of conduct are adhered to by controllers or processors that are not subject to GDPR (*see* article 40, para 3, GDPR), the EDPB have also to verify if there are appropriate safeguards. So far as the EDPB opinion confirms the conformity of the draft code or its amendment or extension, the EDPB will forward its opinion to the Commission. Finally, the Commission can establish that the code, the amendment or the extension has general validity within the EU and

---

para 2, GDPR: « (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79».

[19] In any case, the adoption of codes of conduct is not the only instrument made available to data controllers and data processors in order to comply with the accountability principle. These should in fact be considered together with other important means, such as the DPIA (art. 35, GDPR) and the certifications (art. 42, GDPR).

there the Commission provides adequate publicity for the approved codes with general validity and the EDPB collects all the codes of conduct, amendments and extensions approved in a register and makes them public by appropriate means.

On 12 February 2019, the "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679", [20] which are the first guidelines on codes of conduct, were adopted by the EDPB to promote and encourage the development of these self-regulatory systems, that to date is implemented to a limited extent. The merit of these guidelines is that they shed light on the procedures and rules relating to the presentation, approval and publication of codes of conduct at both national and European level. The guidelines also provide indications on the minimum contents necessary for the codes of conduct to be accepted by the competent DPA.

It is important to underline that the codes of conduct are not new to the Italian legal system. Before the adoption of the GDPR, the Italian privacy code, under article 12, provided the possibility of signing codes of ethics and good conduct (in Italian "codici di deontologia e buona condotta"). The codes of ethics and good conduct approved were deontological rules (in Italian "regole deontologiche") contained in Annex A of the Italian privacy code and the same have recently been reviewed by the Italian DPA and published in the Italian Official Journal (as provided under article 20, para 4, legislative decree no.101 / 2018). Specifically, the updated texts were published in the Italian Official Journal in January 2019 and concern: the processing of personal data in the exercise of journalistic activity, the archiving in the public interest or for historical research, the statistical or scientific research purposes, carrying out defensive investigations or asserting or defending a right in court. [21]

As the facts show, in Italy the codes of conduct are very important and currently the Italian DPA has approved several, defining them deontological rules.

---

[20] The Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 of the EDPB are freely available here: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it.

[21] More precisely currently there are seven Italian codes of conduct attached to the Italian privacy code: A.1. Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica; A.2. Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica; A.3. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale; A.4. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica; A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti; A.6. Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria; A.7. Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale.

Article 2 *quater* of the Italian privacy code requires the Italian DPA to promote the adoption of deontological rules and verify their compliance with current regulations, especially for activities that involve the processing of data necessary for the fulfillment of legal obligations (article 6, paragraph 1 letter c), GDPR), for the execution of a task of public interest or connected to the exercise of public authority (Article 6, paragraph 1, letter e), GDPR) and for data genetic and health related (Article 9, paragraph 4, GDPR).

4. Main data protection topics for DPOs

After analysing the sources of law on data protection and the principal innovations resulting from the data protection reform, this paragraph illustrates the main data protection topics regulated in the abovementioned sources of law that a DPO should know to better perform his of here tasks. Such subjects have been examined to produce a list of topics and sub-topics for training of DPOs. More precisely, it is the result of a study conducted for defining the topics of interest for a DPOs' training course within TAtoDPR project, better illustrated in the table below.

The proposed list of topics has followed the guidelines provided by national DPO Certification Bodies and the national Data Protection Authorities in Spain, in Italy and in the United Kingdom, intending to produce courses which could benefit from certification schemes. [22]

As we will try to demonstrate the data protection reform has embarked on a new march to the already articulated discipline envisaged at European and national level. In fact, to respond to technological developments and new models of economic growth (recital 6, GDPR), the GDPR has provided technologically neutral protection rules, which apply regardless of the technique used and the automation applied (recital 15, GDPR). Furthermore, the GDPR modifies the basic system of the processing of personal data, proper to Directive 95/46/EC and national legislation, about the organizational and business models and the obligations of the data controller and data processor. However, at the same time, the fundamental principles related to the data subjects, and their rights and du-

[22] In particular, the Spanish Data Protection Authority has published the general guidelines that regulate the Certification Scheme for the DPO figure. Spanish Data Protection Authority has published the general guidelines are available at: http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/SCHEME_AEPD_DPD.pdf. The Spanish DPO Certification Body is ANF (www.anf.es). The DPO certification is regulated by the ISO standards and has an international recognition. In Italy, this certificate will be issued in compliance with the regulation UNI 11697:2017.

ties are conserved, even with some modifications.

With the GDPR, administrative obligations have been reduced, despite the reintroduction of obligations to fill documents related to the processing of personal data (eg. Records of processing activities, under articles 30, GDPR). Furthermore, the processing of personal data, which are carried out according to the law, are conducted "at risk" of the data controller and, eventually data processor.

Moreover, the European Regulation does not affect the existing oligopolistic market structure in the field of personal data even though does not hinders the entry of new players (expressly provided by GDPR, as the DPO, or developed in the practise, as the person in charge for the processing) or formally encourages the subdivision of tasks between the existing figures (eg. sub-data processors in the case in which the data processor engages another data processor). In this light, a very important measure introduced for the protection of personal data concerns the appointment of the new control figure represented by the Data Protection Officer (Articles 37 ff., recital 97, GDPR). The DPO is a physical person, who requires a third-party position and acts as a consultant for the data controller or the data processor, in order to ensure correct management in companies and institutions and act as a contact point between the Authorities. The figure of the DPO is mandatory for public subjects, in the case of treatments that require regular and systematic monitoring on a large scale or in the case of special categories of data (pursuant to Article 9, GDPR) or personal data relating to criminal convictions and offences (pursuant to Article 10, GDPR).

The GDPR does not fail to identify a series of preventive measures that the data controller must adopt, even if there are provisions that overturn the duty of data protection on the organization and on technological instruments. In this way, we can consider the Data Protection Impact Assessment, abbreviated as DPIA (recitals 84 ff. and articles 35 ff., GDPR) applicable in case of high risk for data subject's rights and freedoms. Another important preventive measure is the design of systems aimed at minimizing the use of personal data (data protection by design and data protection by default, under article 25, GDPR), which are technical and organizational measures aimed at reducing the risk for personal data (such as pseudonymisation).

The preventive measures listed are intended to make accountable the behaviour of the data controller (accountability principle, under articles 2 and 24, GDPR) concerning the adoption of procedures able to avoid data risks, in order to prevent high administrative fines. On the other hand, the codes of conduct (articles 40 and 41, GDPR) and the certification mechanisms issued by a qualified body or by the data protection authority (article 42 and 43, GDPR)) can be interpreted in the sense of an improvement of the organizational data protection models (article 35 ss., GDPR).

In the same direction of the preventive measures, go the affirmation of data subject's rights stated in the GDPR (the right to be forgotten, under article 17, GDPR and the right to data portability, under article 20, GDPR), as well as, the uniform regulation within the single market of data processing of those who are on the territory of the European Union, guaranteed by the European Data Protection Board (article 68, GDPR), which is in addition to the existing European Data Protection Supervisor and national Data Protection Authorities.

Anyway, for the case in which the *ex ante* protection is not enough, GDPR introduced high administrative fines (articles 83 ff., GDPR), up to 2% or 4% of the annual worldwide turnover of the previous year[23]. The GDPR also provides compensation for damages (article 82, GDPR), but without significant innovations in comparison with the previous regulatory framework (Directive 95/46/EC)[24]. The tightening of administrative sanctions can be interpreted in the sense of increased deterrence. Finally, even if the GDPR does not expressly provide penalties, as already said it admits the possibility for Member States to establish other penalties in case of non-compliance with GDPR (art. 84), as well as other administrative fines for the infringements of national rules adopted within the limits of the GDPR (Recital 148).

---

[23] More precisely, chapter VII of the GDPR regulates Remedies, liability and penalties. In this context, art. 83 GDPR distinguishes two groups of administrative fines: minor fines and major fines. Indeed, it provides minor fines (so to speak) up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year in case of the infringements of the obligation imposed on: (a) the data controller and the data processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43 GDPR; (b) the certification body pursuant to Articles 42 and 43; (c) the monitoring body pursuant to Article 41(4). The same articles impose major administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year in case of the infringements of: «(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1)».

[24] Anyways, in Italy, the d.lgs. no. 101/2018, provide the express repeal of the art. 15 of Italian privacy code, which has regulated the right to compensation for data breach. This is the reason why, also in Italy art. 82 of the GDPR is the new fundamental rule on civil liability in the processing of personal data and the consequent right to compensation for damage. Anyways, from an in-depth analysis of the case-law at European and national level, emerged the difficulty of proving the damage coming from the unlawful processing of personal data in the field of civil liability. This study is a work conducted by the Research Center of European Private Law (ReCEPL) at Suor Orsola Benincasa University of Naples, which will be published separately, and it took into account both case law on art. 15 of the Italian privacy code and these on art. 82 of the GDPR.

The above-mentioned regulatory choices reveal an approach aimed not to prevent the increasingly massive production and processing of personal data made by new technology and techniques that allow the multiplication of the data themselves and of their processing, but to regulate the processing with mechanisms which have the purpose of minimizing the risks of loss, dispersion and diffusion of personal data, in order to protect the sphere of the data subjects.

Technology (eg. privacy by design, through anonymisation and pseudo-anonymisation)[25] is called upon to regulate technology according to the objectives set by the European legislator, while the legal rules gain their own important role concerning the sanctions. However, it remains to be seen whether the techno-regulation as well as the careful use of the sanctioning power by the DPAs and the national courts will be efficient, performing the desired *ex ante* and *ex post* protection. This problem derives from the fact that, the GDPR does not have much impact on some incoherent approaches, as in the case of automated processing of personal data, including profiling process, that must be the object of timely information, authorisation, and right of opposition (article 22, GDPR). With regard to user profiling, reference should be made to the regulatory provisions according to article 4, n. 4, recitals 32, 60, 63, 70, 71, 72, articles 13, para. 2, lett. f), 14, para. 2, lett. g), GDPR that, however, do not regulate profiling issue completely and protectively because do not provide specific preventing measures (*ex ante* protection) or specific deterrent measures (*ex post* protection).[26]

[25] Privacy by design together with privacy by default are important novelties introduced by the GDPR (art. 25). These are adequate technical and organizational measures which aim to protect the data from unlawful processing. This implies an innovative conceptual approach that requires data controllers to start a project, providing by design and by default the right tools and settings to protect personal data.

[26] In this already very complex context, with regard to profiling process an important role is played by electronic communications, currently regulated under Directive 2002/58/EC on electronic communications (well known as ePrivacy Directive) as well as the Proposal for an ePrivacy Regulation.

Table 1 - Proposed table of topics that a DPO should know [27]

1. The right to privacy and the right to data protection
1.1 The privacy legislation before GDPR in the countries of the European Union, with particular regard to the Italian legal system.
1.2 Privacy and European data protection law: from Directive 95/46/CE to the new EU Regulation 2016/679
1.3 Codes of conduct and certifications applicable to the processing and protection of personal data
1.4 ISO/IEC technical standards and best practices
2. Privacy Principles
2.1 Lawfulness, fairness and transparency
2.2 Purpose limitation
2.3 Accuracy
2.4 Storage limitation
2.5 Integrity and confidentiality
2.6 Accountability
2.7 Data protection by design and by default
3. The rights of data subjects
3.1 Information to be provided when personal data are collected or not collected from the data subject
3.2 Right to update data
3.3 Right to cancellation (right to be forgotten in relation with press freedom)
3.4 Conditions
3.5 Right to limit the processing
3.6 Right to data portability
3.7 Opposition law

[27] This table has been published in one of the Deliverable of the TAtoDPR Project.

3.8 Right not to be subjected to a decision based solely on automated processing, including profiling
4. Legal provisions on the transfer of personal data abroad
4.1 Binding corporate rules (Bcr)
4.2 Privacy Shield
4.3 Third countries, representatives in EU Member States
5. The consent to the processing of personal data
5.1 Consent provision and demonstration of the provision of consent
5.2 Characteristic and condition of informed consent
5.3 Method of acquiring consent
5.4 Silence, inactivity or pre-selection of boxes
5.5 Withdrawal of consent and preventive information
5.6 Freedom to provide consent
5.7 Minimum elements: indication of the data controller and the purposes of the processing
5.8 Consent of children in the information society
5.9 Specific cases: • Processing and consent to processing in the health sector P • Processing necessary to fulfill a contract • Processing required by law • Processing necessary to safeguard the vital interests of the data subject or other natural person • Processing necessary for public interest
6. Data protection impact assessment (DPIA)
6.1 Setting, structure and dynamic value of the GDPR
6.2 Codes of conduct and impact assessment
6.3 Integration of the GDPR with the D.lgs. 196/2003 on the national data protection
6.4 Integration of the GDPR with the D.lgs. 231/01 on the responsibility of the institutions

6.5 Public interest issues
7. Type of personal data
7.1 Type and classification of data
7.2 Problems related to unstructured data (e. g. data analytics, standard K180) – cyber-attack techniques and countermeasures to avoid them.
7.3 Problems related to the size of data sets (for example, big data)
7.4 Anonymized and pseudonymised data
8. The roles
8.1 Data controller
8.2 Data processor
8.3 Data protection officer (included the professional insurance for DPO and national and international certification)
9. The organisation's processes
9.1 (Automated) Decision-making
9.2 Budget and management structures
9.3 Information strategy
9.4 Monitoring and reporting systems and techniques
9.5 Typical key performance indicators (KPIs)
9.6 Version control tools for the production of K49 documentation - skills development methods
9.7 Specific fields • Banking sector • Labour Law • Public administration • Police justice and security • Health system
10. Critical risks for safety management
10.1 Possible security threats

10.2 The impact of legal requirements on information security
10.3 Company security management policy and its implications for customer, supplier and sub- contractor commitments
11. New emerging technologies and privacy
11.1 Distributed systems, Virtualization models, Mobility systems and Data sets
11.2 Internet of things and Big Data
11.3 Cloud computing
1.4 Cookies, web analytics, and other user tracking technologies
11.5 Cyber security
11.6 Bioethics and biological data
12. Responsibilities , Remedies and Penalties
12.1 The possible threats to the protection of personal data
12.1 The possible threats to the protection of personal data
12.3 Liabilities
12.4 Remedies: the claim to a supervisory authority
12.5 Penalties

5. Conclusions

Data are acquiring a huge role in our society and, in some contexts, they are considered a new currency of exchange. Through the development of new technologies, both the production of personal data and the processing of personal data is massively increasing. This brought two major implications. From one side, data are in the condition to shape our lives and in general to handle new way to perform both public services and business. For instance, weather forecasts, marketing strategies, impact on public policies, and so on, could have a higher reliability thanks to personal data available and their manipulation within algorithms. From the other side, data have at the same time impact on privacy, as they could give an unexpected and quite detailed portrait, even indirectly, on data subject. In this scenario is born the need of greater protection of personal data, which required the data protection reform implemented through the GDPR, even if some areas of the data processing remain not entirely regulated and, for

this reason (also on the basis of the recent law proposals), it is conceivable that the European legislator will intervene again in the matter.

Currently, to provide a strong *ex ante* protection of personal data, GDPR took the decision, among the others, to introduce in certain kinds of public entities and companies a privacy professional specifically dealing with privacy issues referred to data management: the Data Protection Officer (DPO). This figure is designed by the data controller or the data processor and has to perform specific tasks and functions, related to the processing of personal data regulated under articles 37 and following of the GDPR. The DPO is required to be in a third-party position and acts as a consultant for the data controller or the data processor, ensuring correct management in companies and public entities and act as a contact point between the DPAs. The figure of the DPO is mandatory in different cases so that it is one of the major fields of specialization for professionals since it is a very popular figure in the labour market. This is one of the reasons why it is necessary to provide an accurate preparation for those who intend to take on the DPO role.

The hard and soft law on data protection as well as the list of topics deepened in this paper represent a basis in the increase of DPO training activity. They serve as the main support and working tool for the design and implementation of DPO knowledge. Starting from this point, DPO will be able to develop his consciousness and implement his skills.