JOINT CONTROLLER AGREEMENT UNDER GDPR

Valentina Colcelli, PhD, Researcher of National Research Council
IFAC Institute
Via Madonna del Piano, 10 Sesto Fiorentino, Firenze, Italy
valentina.colcelli@cnr.it

ABSTRACT

The GDPR obliges organisations to keep watch for potential instances of joint controllership of personal data. Where those instances arise, organisations must enter into suitable "arrangements" that apportion data protection compliance responsibilities between joint data controllers. The controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. But, f.i. in the case of the case of a Biobank, more than one public bodies are the controllers of personal data, and their processing takes place in an intra-group context.

The paper will analyse elements established by art. 26 GDPR for Joint Controller Agreement for managing personal data under GDPR, the respective roles and relationships of the joint controllers vis-à-vis the data subjects, as well as responsibility and liability of controllers and processors.

Keywords: *Joint controllership, Personal data, Joint Controller Agreement, Joint controller liability*

1. INTRODUCTION

The paper aims at assessing the elements established by art. 26 GDPR for Joint Controller Agreement, respective roles and relationships of the joint controllers *vis-à-vis* the data subjects, as well as responsibility and liability of controllers and processors.

GDPR regulates the joint ownership of the data treatment (art. 26) and requires controllers to specifically define (by an act legally valid under national law) the respective scope of responsibility and tasks with particular regard to the exercise of the rights of the persons concerned, who have the opportunity to apply indifferently to any of the controller operating jointly.

The data controller is defined by GDPR (art. 4 n. 7) "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member

State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". As controller, we mean the legal entity in its entirety, not the legal representative or head of the legal entity. Thus, the controller could be a professional, as well as a legal person (private or public body), association, multinational enterprise, able to determine by itself purposes and means of the processing of personal data, not for its individual uses. Just only in the presence of both of the requirements mentioned above, it is possible to identify a controller, or joint controllers if the data of the owners operate jointly.

About any processing activity, it is possible for more than one entity to be the controller, where the processing takes place in an intra-group context (f.i. research projects founded on EU grants, biobanks or others). "However, a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46. Furthermore, the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned"[1].

The GDPR obliges organisations to keep watch for potential instances of joint controllership.

Where those instances arise, organisations must enter into suitable "arrangement" that apportion data protection compliance responsibilities between joint controllers.

Data controllers should carefully assess the existence of possible situations of joint ownership (see, in this regard, the indications provided f.i. by the Italian Data Protection Authority in various measures, including web doc. no. 39785)[2], being obliged in this case to enter into the internal agreement referred to in article 26, paragraph 1, GDPR.

The Joint controller agreement is a new form of "legal relationship", foreseen for the first time by the GDPR. It offers many opportunities to regulate legal arrangement in the most diverse economic sectors. Particularly relevant will be the definition of the respective functions of communication of the information referred

---

1 Case C25/17 , *Tietosuojavaltuutettu vs Jehovan todistajat — uskonnollinen yhdyskunta*, [2018] ECLI 551 par. 68 and 69

2 Italian Data Protection Authority, *Titolare, responsabile, incaricato - Precisazioni sulla figura del 'titolare' - 9 dicembre 1997*, doc. web. n. 39785 Retrieved from [https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785access] Accessed 20.02.2019

to in Articles. 13 and 14 to the data subjects, to whom the data controllers are subject.

An essential summary of the agreement must be made available to the interested parties, also in compliance with the principle of transparency[3]. The interested party, regardless of the provisions of the agreement between the various joint holders, may exercise their rights, provided for in the regulations, against and against each holder.

The advantages offered by this agreement are many: it is important to point out that, as an alternative to the appointment of the controller, the holder will be able to negotiate a joint ownership agreement with the partner and, by establishing mutual obligations and responsibilities, avoid, for example, an audit of the controller that would otherwise be necessary. In this respect, it will be essential to negotiate the obligations and responsibilities of each party in order to establish a useful and not counter-productive agreement.

The chapter is organised as follows: in Section 2 we provide an overview on the meaning of controllers in the light of the joint controllership; the Section 3 offers some examples how joint controllers are identified by the European Commission, the EU Court of Justice or by Article 29 Working Party, also because it is not so easy to understand when the controllers are joint controllers; Section 4 identifies requirements that must be included in all data processing agreements and Section 5 recognizes how liability should be apportioned between the joint controllers, to guarantee the data subjects in the perspective of EU data protection law. The Section 6 concludes.

2. THE ESSENCE OF THE ARRANGEMENT: PURPOSES, AND MEANS OF THE PROCESSING OF PERSONAL DATA.

GDPR requires to the controller to be responsible for making sure all privacy principles are adhered to[4]. "The data controller must adhere to what is stipulated under Article 5 GDPR, which states that personal data must be processed lawfully, fairly, and in a transparent manner (Blawfulness, fairness and transparency). (…) The personal data must be collected for specified, explicit, and legitimate purposes

[3] See generally Custers, B.; Sears, A. M.; Dechesne, F.; Georgieva, I.; Tani T.; Van der Ho, S., *EU Personal Data Protection in Policy and Practice*, T.M.C. Asser Press, The Hague, 2019; Malgieri G.; Custers B., *Pricing privacy – the right to know the value of your personal data*, Computer Law & Security Review, *Vol.* 34, No. 2, 2018, pp. 289-303; Pizzetti, F., *Privacy e il diritto europeo alla protezione dei dati personali, II: Il Regolamento europeo 2016/679*, G. Giappichelli, Torino, 2016, pp. 6-9

[4] Emili A. M., *Data Officer Protector*, A. Bartolini, R. Cippitani, V. Colcelli (Eds) Dictionary of Statuses within EU law, Springer International, Cham, 2019, p. 121

(purpose limitation) and must be adequate and necessary in relation to the purposes for which it is collected (data minimisation)" [5].

The controller and the joint controllers have to monitor also "the behaviour of data subjects" as mentioned in Recital 24 of GDPR. This activity clearly includes all forms of tracking and profiling on the internet. "However, the notion of monitoring is not restricted to the online environment, and online tracking should only be considered by way of example. WP29 interprets 'regular' as meaning one or more of the following: ongoing or occurring at particular intervals for a particular period; recurring or repeated at fixed times and constantly or periodically taking place. Whereas, WP29 interprets 'systematic' as meaning one or more of the following: occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection and carried out as part of a strategy". [6]

Where two or more controllers jointly determine the purposes, and means of the processing of personal data, they are joint controllers (Rec.79; Art.4 (7), and Art.26). Core activities of the controller or the processor are intended to be 'the key operations necessary to achieve the controller's or processor's goals'; however, they should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's[7] activity[8].

A company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller, so if the determination is made with one or more organisations, the latter are joint controllers.

Because of the GDPR, Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. This means that both controllers will have to take into account the jointly determined nature, scope, context and purpose of the processing, as well as the risks to which each party is exposed, in terms of probability and severity, and to determine appropriate technical and organisational measures to ensure and be able to demonstrate that the processing complies with the Regulation.

---

5 Niamh Clarke G., *et. al., GDPR: an impediment to research?,* Ir J Med Sci, 2019, Retrieved from [https://doi.org/10.1007/s11845-019-01980-2] Accessed 08.02.2019

6 Emili, *op. cit.*, note 4, p. 122

7 *Ibid.*

8 'Processor' shall mean a natural or legal person, public authority, agency or anyother body which processes personal data on behalf of the controller (Definitions of 'controller' and 'processor' in Article 2 (d) and (e) of Directive 95/46/E).

It is necessary, that is, the exact and explicit determination of the aims of the treatment, so much so that in the event that it is a public body that gives the rules setting up and regulating the institution and the rules governing the may establish the purposes for which this is done by the implicit definition of the purposes is not sufficient to legitimize the treatment. The arrangement may represent a contribution to the documentation of the legitimacy of the purpose which in any case, it must be made explicit, thus excluding the possibility that they could ever settle *per relationem*[9].

3. JOINT CONTROLLERS, SOME EXAMPLES.

"Multiple actors involved in processing personal data is naturally linked to the multiple kinds of activities that according to the Regulation and the former Directive may amount to 'processing', which is at the end of the day the object of the joint control"[10].

Anyway, it is not so easy to understand when the controllers are joint controllers.

The European Commission refers this example: "Your company/organisation offers babysitting services via an online platform. At the same time your company/organisation has a contract with another company allowing you to offer value-added services. Those services include the possibility for parents not only to choose the babysitter but also to rent games and DVDs that the babysitter can bring. Both companies are involved in the technical set-up of the website. In that case, the two companies have decided to use the platform for both purposes (babysitting services and DVD/games rental) and will very often share clients' names. Therefore, the two companies are joint controllers because not only do they agree to offer the possibility of 'combined services' but they also design and use a common platform."[11].

Among the others, Article 29 Working Party suggests the following examples that could be qualified as joint controllers:

---

9 *Contra* Navarretta E., *Commento sub art. 11 del D.lgs., 30 giugno 2003, n. 196*, in: Bianca C.M.; Busnelli F.D., (eds.) La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della privacy»), I, Cedam, Padova, p. 322

10 Article 29. Working Party Opinion 1/2010 (adopted on 16 February 2010, reference number 00264/EN/WP 169) retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] Accessed 08.02.2019

11 *What is a data controller or a data processor?* retrieved from [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en] Accessed 15.02.2019

- "Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called "household exception"[12].

- E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit. These controllers, among other obligations, will have to ensure that the system to transfer personal data from the user to the public administration's system is secure, since at a macro-level this transfer is an essential part of the set of processing operations carried out through the portal[13].

In the opinion of the Court of Justice of the EU decided in Case C-210/16 *Wirtschaftsakademie*[14], Facebook and the administrator of a fan page created on Facebook are joint controllers under EU data protection law. The Court of Justice in this judgment describes because of the concept of 'controller' encompasses the administrator of a fan page hosted on a social network: (15) "Fan pages are user accounts that can be set up on Facebook by individuals or businesses. To do so, the author of the fan page, after registering with Facebook, can use the platform designed by Facebook to introduce himself to the users of that social network and to persons visiting the fan page, and to post any kind of communication in the media and opinion market. Administrators of fan pages can obtain anonymous statistical information on visitors to the fan pages via a function called 'Facebook

---

12 Article 29 Working Party's Opinion 5/2009 on online social networking, adopted on 12 June 2009 (WP 163), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf] Accessed 08.02.2019

13 Article 29. Working Party Opinion 1/2010 (adopted on 16 February 2010, reference number 00264/EN/WP 169) retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] Accessed 08.02.2019, p. 23

14 Case C-210/16 *Wirtschaftsakademie- Schleswig-Holstein* [2018] ECLI 388

Insights' which Facebook makes available to them free of charge under non-negotiable conditions of use. That information is collected by means of evidence files ('cookies'), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on other media of visitors to fan pages. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened. According to the order for reference, neither *Wirtschaftsakademie* nor Facebook Ireland Ltd notified the storage and functioning of the cookie or the subsequent processing of the data, at least during the material period for the main proceedings."

Thus, the question is whether or not an entity to be held liable in its capacity as administrator of a fan page on a social network where the rules on the protection of personal data are infringed, because it has chosen to make use of that social network to distribute the information it offers: "30. In the present case, Facebook Inc. and, for the European Union, Facebook Ireland must be regarded as primarily determining the purposes and means of processing the personal data of users of Facebook and persons visiting the fan pages hosted on Facebook, and therefore fall within the concept of 'controller' within the meaning of Article 2(d) of Directive 95/46, which is not challenged in the present case. (…) 32. It appears that any person wishing to create a fan page on Facebook concludes a specific contract with Facebook Ireland for the opening of such a page, and thereby subscribes to the conditions of use of the page, including the policy on cookies, which is for the national court to ascertain. (…) 35. While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account. 42 In those circumstances, the recognition of joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that page contributes to ensuring more complete protection of the rights of persons visiting a fan page (…)".

Scholars identify also the management of research data like a joint controllership in the case i.f. of observational research, when patient data derive from different healthcare systems[15] or biobank like the Human genetic databases (HGD) that

[15] Borghi, M., *Individual rights and property rights in human genetic databases: a common-law perspective*, in: Rainer, A.; Cippitani R.; Colcelli V. (eds.), Genetic Information and Individual Rights, Universität

are essential facilities for medical research[16]: "in that case, the custodian of the centrally assembled research data should be the sole controller, and data transfer agreements (DTAs) should regulate the processing through that database. The data protection officer of the receiving centre should assure that the conditions are indeed met, next to potential other governance mechanisms of the project such as decision procedures about the use of the database for specific protocols when applicable."[17]

4. TERMS OF THE ARRANGEMENT BETWEEN JOINT CONTROLLERS.

GDPR imposes significant specific requirements that must be included in all data processing agreements. The contract to comply with the elements established by art. 26 GDPR, has to be characterised as follow:

A) It has to establish the respective responsibilities between the controllers for compliance with the obligations under GDPR.

B) It has duly to reflect:

   i) the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects.

   ii) the protection of the rights and freedoms of data subject.

C) It may designate a contact point for data subjects.

D) It has to determine the clear allocation of the responsibilities and liability of controllers and processors under GDPR.

The essence of the arrangement shall be made available to the data subject. The essence of the Joint controller agreement is a clarify distribution of control.

Anyway, at national level only just two Data Protection Acts provide some general guidelines on joint controllership: the Norway Act of 15 June 2018 no. 38, and Belgican Act of 30 July 2018 Federale Overheidsdienst Justitie, Federale Overheidsdienst Binnenlandse Zaken En Ministerie Van Landsverdediging "*Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van*

Regensburg, Regensburg, 2018, p. 120

16 See generally Tutton, R.; Oonagh, C. (eds.), *Genetic Databases: Socio-ethical issues in the collection and use of DNA*, Routledge, London and New York, 2004; Häyry M. *et al.*, *The Ethics and Governance of Human Genetic Databases. European Perspectives,* Cambridge University Press, Cambridge, 2007; Elger, B., *Ethical Issues of Human Genetic Databases: A Challenge to Classical Health* , Routledge, London and New York, 2012

17 van Veen E.-B., *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, European Journal of Cancer, *Vol.* 104, 2018, p. 75

persoonsgegevens"[18]. This means that for the legal operators it is not so easy to work on a good construction of a joint controllers agreement because of not any deep analysis by the national legislators about its requirements.

Nevertheless, following the art. 26, we can summarise how by the joint agreement, the joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under GDPR.

The arrangement clauses especially have to explicit in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 GDPR to the data subjects. The articles mentioned above require the information to be provided where personal data are collected from the data subject (art.13) and the information to be provided where personal data have not been obtained from the data subject (art.14).

At the same time, the article 26 invites to clarify to whom the data controllers are subject, and the definition of the respective functions of communication of the information.

The responsibility and the liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities have to be determinate. The arrangement requires a clear allocation of the responsibilities under the GDPR, "including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller" (Recital 79 EU GDPR).

The above-mentioned clauses are the core of the arrangement because explicitly established by the DGPR.

The clauses list on Art. 26 GDPR opens the question about what happens if one of these clauses is not planned in the text. "With respect to data subjects, it is important that transparent information is provided to the intended subjects by the data controller on the methods by which their data will be processed"[19], so the set of information that must be provided to data subject seems to be a mandatory requirement and compulsory to reach the GDPR goal.

---

[18] Belgian Act in the art. 52. "(…) Mutual arrangements shall establish the respective responsibilities of the joint controllers in a transparent manner, in particular with regard to the exercise of the rights of the data subject and to provide the information referred to in Articles 37 and 38, unless their respective responsibilities have been established by the law, the decree, the ordinance, the European regulations or the international agreement. A single point of contact for the parties involved can be designated in the mutual arrangement"

[19] Niamh Clarke, *et al., op. cit.,* note 5

GDPR seems to be a communitarian compulsory rule, especially the transparent data processing is mandatory in private enforcement of the law. If so, it could have a huge effect on the enforcement of the GDPR.: f.i under the Italian legal system, the joint controller's agreement contrary to mandatory rules on transparent data processing information would be void (art. 1418 Italian Civil code). This means that void contracts have neither binding force nor legal effectiveness and that the nullity may be claimed by anyone, and it can also be declared by a national court.

Anyway, it is possible to insert other kind of clauses to well-equip the agreement, f.i. the possibility for each party A) to terminate the Agreement (with or not with immediate effect) if the other party not shall comply with all the obligations imposed on a controller under the GDPR in the performance of its obligations under the Joint Controller Agreement; B) to ascertain that provisions of Agreement shall continue to apply to any personal data in the possession of either party which was covered by the Agreement eventually expired; C) to foreseen a mutual assistance in complying with all applicable requirements of the GDPR; D) to establish how and if implementing appropriate technical and organisational security measures to protect personal data in possession to other party; E) to inform each other of any data breaches; F) to establish clear rules to ensure information will not be processed outside of EU without the appropriate security measures and how the all partners must be informed of this intent with sufficient notice in writing.

Always, data subjects are entitled to enforce their rights in respect of and against each of the controllers, so the essence of the arrangement shall be made available to the data subject.

In particular, it could be important, but not necessary, to identify the "contact point for data subjects" in order to exercise the rights provided for by the Regulation.

5. JOINT CONTROLLER LIABILITY.

In the joint controllers arrangement, roles and responsibilities must be allocated. "Unfortunately, due to the multiplicity of possible arrangements, it is not possible to draw up an exhaustive 'closed' list or categorization of the different kinds of joint control. (….). In the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared." [20]

[20] Article 29. Working Party Opinion 1/2010 (adopted on 16 February 2010, reference number 00264/EN/WP 169) retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] Accessed 08.02.2019, p. 21

The Joint controllers can be given if one cooperation partner decides on the purposes of the data processing, with the other deciding freely on the means of the data processing. The judgment C-210/16 *Wirtschaftsakademie* remembers us how the shared responsibility is not always equal: it depends on the stage of the processing the joint controller is involved in and on the actual control it has over the processing. At the same time the judgment above mentioned seem to interpret concept of being "jointly responsible" as equivalent to the concept of "joint controllership" as laid down in Article 26 GDPR, opening the door for a broader interpretation of the term "Joint Control".

Also if the broad interpretation of the definition of a controller opens the problem for the "delineation of responsibility so far does not follow from the broad definition of a controller. The danger of that definition being too broad is that it results in a number of persons being co-responsible for the processing of personal data."[21]. Thus, according to Advocate General Bobek, the controllership should be interpreted with respect to operations of processing not in relation to "processing" in general (globally to all operations).

Arrangement ascertains the responsibility and liability of controllers and processors, anyway question of how liability should be apportioned between the joint controllers, while important to organisations, is a secondary question from the perspective of EU data protection law. With regard to controllers' liability Advocate General Bobek states "a (joint) controller is responsible for that operation or set of operations for which it shares or co-determines the purposes and means as far as a given processing operation is concerned. By contrast, that person cannot be held liable for either the preceding stages or subsequent stages of the overall chain of processing, for which it was not in a position to determine either the purposes or means of that stage of processing." "(…) Through a broad definition of the concept of 'controller', effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"[22].

---

[21] Advocate General, Michal Bobek, Opinions delivered in case Fashion ID, C-40/17, Retrieved from [http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&doclang=EN] Accessed 05.05.2019

[22] Case C25/17 , *Tietosuojavaltuutettu vs Jehovan todistajat — uskonnollinen yhdyskunta*, [2018] ECLI 551 par. 66

That's because of each joint controller is liable for the entirety of the damage, although national law may apportion liability between them (Liability of joint controllers, Rec.79, 146; Art.26(3), 82(3)-(5)). Where liability arises in a joint controllership scenario, EU data protection law's primary focus is on ensuring that the data subject is protected. "Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage." (Recital n. 146).

"The GDPR makes joint controllers fully liable. Once 'full compensation' has been paid to the affected data subject(s), joint controllers may recover damages from one another."[23] According to article 82 paragraphs 2 and 3, because of a data subject can apply to ask for damage in the case of the joint-controllers involved in the data treatment, data subject has to put in the condition to know the internal arrangement as above explained.

If one joint controller has paid full compensation, it may then bring proceedings against the other joint controllers to recover their portions of the damages (art. 82, paragraph 5).

The full responsibility of each controllers established by the Regulation, reproduces rules already existent in the internal legal systems, so the data subject will not be affected by the will not be damaged by insolvency, disappearance or liability for the infringement[24]: see for instance the art. 2055 in the Italian civil code establishes that "if the act causing damage can be attributed to more than one person, all are jointly and severally liable for the damages. The person who has compensated for the damage has recourse against each of the others in proportion to the degree of fault of each and to the consequences arising therefrom." So, in case of doubt "the degree of fault attributable to each is presumed to be equal." In the light of European harmonization, also the French jurisprudence[25] "does not accept that a victim may be undercompensated just because one or several of the tortfeasors may be unknown". If several controllers "may have caused the damage, they can be made liable under one of the following doctrines: fault based liability (*faute commune, faute* collective), if acting as a group and guilty of a collective fault"[26]. Under the German tort law,

---

23 Detlev, G.; Hickman T., *Obligations of controllers*, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law, 2019, retrieved from [https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection] Accessed 09.02.2019

24 Gambini M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in: Di Cuffaro, V.;, D'orazio R.; Ricciuto V., (eds.), I dati personali nel diritto europeo , Turin, Giappichelli, 2019, p. 1026

25 Cass. Civ. 2, 2 April 1997, Bull. II, no. 112

26 Moréteau O., *French Tort Law in the Light of European Harmonization*, Journal of Civil Law Studies, *Vol.* 6, 2013, p. 792

the Civil code provides "that several tortfeasors who have caused the same harm are jointly liable (830, 840 par. 1 BGB). The Code provisions still distinguish between different kinds of joint torfeasors although the consequence is identical for all, namely joint liability. Joint liability means that the victim is entitled to claim (and sue) compensation of the full damage for each tortfeasor although the whole compensation ha to be paid only once (see 421 BGB). As a well a judgment can be enforced against of anyone of the tortfeasors at the victim's discretion. If one torfeasor ha satisfied the claim in full it is for him to sue the others for eventual redress and to bear the accompanying procedural and insolvency risk."[27]. In the Portuguese tort law the article 490 states "if there are multiple actors, instigators or collaborators of the wrongful act, all of them are liable for the damage caused by them". "Art. 497 prescribes the solidarity regime in the tort law"[28]. The fully responsibility draws by the GDPR is another step beyond on the way for the unification of the Unification of tort law among the Member States.

Anyway, according to the general principal of the European tort laws, the joint responsibility doesn't mean any exception to the principle of liability, so close to the principle of joint responsibility survives differentiated responsibility. This is the meaning of "Recital" n. 146: "the controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage". For freeing oneself from responsibility requires positive proof that one has employed every cure or valid measure to prevent the harmful event. It is therefore not enough negative proof that they have not infringed any provision of law or regulation or otherwise the rules of common prudence. Anyway, where controllers or processors "are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured", if the subjects will receive full and effective compensation for the damage they have suffered.

The right to compensation for material (actual loss or lost profits) or non-materialdamages (compensation for harm inflicted) on grounds of infringement on the legislation relating to the processing of personal data. Anyway, the concept of

---

27 Magnus U., *Multiple tortfeasors under the German Law*, in: Rogers W. V. H.; van Boom W.H. (eds.), Unification of Tort Law: Multiple Tortfeasors, Kluwer Law International, Netherland, 2004, p. 89

28 Pereira Dias, A.G, *Portugese tort law: a comparison with the Principles of European Tort Law*, Conference Paper, 2004, p. 461, retrieved from [https://estudogeral.sib.uc.pt/bitstream/10316/2563/1/European_Principles_Tort_Law_Portugal.pdf] Accessed 10.05.2019

damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of the GDPR (Recital 146).

The conduct that is considered suitable to integrate the above-mentioned case and from which damage may be caused to the owner of the personal data, are those indicated by the art. 6 of the GDPR and more in general because of the infringes the GDPR, that also includes processing that infringes delegated and implementing acts adopted in accordance with the Regulation and Member State law specifying rules of GDPR (see. Recital 146).

The Processing data, indeed, shall be lawful "only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."[29]

Further hypotheses of conduct suitable for causing damage can be inferred from art. 6, which refers to codes of conduct of different categories including[30] f.i. journalists, as well as codes of conduct for data users' personal data for historical, sta-

[29] Art. 6 Reg. (EU) 2016/679

[30] See Cippitani, *Genetic research and exceptions to the protection of personal data*, in: Renair, A.; Cippitani, R.; Colcelli, V. (ed.) Genetic Information and Individual Rights, Universität Regensburg, Regensburg, 2018, p. 78

tistical or other statistical purposes, for information systems operated by private entities in relation to consumer credits, reliability and punctuality in payments and in relation to the processing of data collected for private investigations.

6. CONCLUSION

If under the GDPR, organisations are obliged to demonstrate that their processing activities are compliant with the Data Protection Principles (Rec.85; Art.5(2) and Rec.74; Art.24 GDPR), an arrangement between joint controllers can help organisations and organisms to demonstrate compliance with all the principles of the regulation: principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality.

As matter of fact, the core of the joint controller agreement are the contractual clauses able to clarify distribution of control and the responsibility and liability of controllers. The art. 26 GDPR requirements can support the joint controllership for data to remain manageable and transparent, especially beyond that and with controllers from member states with different background regimes, where it is joint controllership could become "unmanageable and insufficiently transparent for the data subjects" [31].

At same time, arrangement referred to in paragraph 1 of the art. 26 GDPR "shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects" and "the essence of the arrangement shall be made available to the data subject".

So, the latter has to permit a generalized control on the function of the agreement to stress - on EU dimension - the value of individual control or informational self-determination. "Now that we are living in the GDPR era, one thing is for sure, the increased enforcement power and higher maximum fines, plus the enhanced awareness of data subjects' rights and their ability to exercise those rights means that controllers and processors will be held to account for their processing activities now more so than ever."[32]

---

[31] van Veen E.-B., *op. cit.* note 16, p. 75

[32] Pantlin Nick, Wiseman Claire, Everett, Miriam, *Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR*, Computer law & Security review, 34, 2018, p. 885.

REFERENCES

BOOKS AND ARTICLES

1. Borghi M., *Individual rights and property rights in human genetic databases: a common-law perspective*, in: Rainer, A.; Cippitani, R., Colcelli V. (eds.), Genetic Information and Individual Rights, Universität Regensburg, Regensburg, 2018, p. 120
2. Cippitani, *Genetic research and exceptions to the protection of personal data*, in: Rainer, A.; Cippitani, R., Colcelli V. (eds.), Genetic Information and Individual Rights, Universität Regensburg, Regensburg, 2018, p. 78.
3. Custers, B.*, et al., EU Personal Data Protection in Policy and Practice*, T.M.C. Asser Press, The Hague, 2019
4. Elger B., *Ethical Issues of Human Genetic Databases: A Challenge to Classical Health*, Routledge, London and New York, 2012
5. Emili A. M., *Data Officer Protector*, in: Bartolini, A.; Cippitani, R.; Colcelli, V. (eds.), Dictionary of Statuses within EU law, Springer International, Cham, 2019, p. 121
6. Gambini M., *Responsabilità e risarcimento nel trattamento dei dati personali*, Di Cuffaro V.; D'orazio, R.; Ricciuto V. (eds.), I dati personali nel diritto europeo, Turin, Giappichelli, 2019, p. 1026
7. Häyry M. *et al.*, *The Ethics and Governance of Human Genetic Databases. European Perspectives*, Cambridge University Press, Cambridge, 2007
8. Magnus, U., *Multiple tortfeasors under the German Law*, in: Rogers W. V. H.; van Boom W.H. (eds.), Unification of Tort Law: Multiple Tortfeasors, Kluwer Law International, Netherland, 2004, p. 89
9. Malgieri G.; Custers B., *Pricing privacy – the right to know the value of your personal data*, Computer Law & Security Review, *Vol. 34*, No. 2, 2018, pp. 289-303
10. Moréteau O., French Tort Law in the Light of European Harmonization, Journal of Civil Law Studies, *Vol.* 6, 2013, p. 792
11. Navarretta E., *Commento sub art. 11 del D.lgs., 30 giugno 2003, n. 196*, in: Bianca C.M.; Busnelli F.D. (eds.), La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della privacy»), I, Cedam, Padova, p. 322
12. Pantlin N.; Wiseman C.; Everett, M., *Supply chain arrangements: The ABC to GDPR compliance —A spotlight on emerging market practice in supplier contracts in light of the GDPR*, Computer law & Security review, *Vol.* 34, 2018, p. 885.+
13. Pizzetti, F., *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, G. Giappichelli, Torino, 2016, p. 6
14. Tutton R.; Corrigan O., (eds.), *Genetic Databases: Socio-ethical issues in the collection and use of DNA*, Routledge, London and New York, 2004
15. van Veen E.-B., *Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate*, European Journal of Cancer, *Vol.* 04, 2018, p. 75

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C- 25/17 Tietosuojavaltuutettu vs Jehovan todistajat — uskonnollinen yhdyskunta [2018] ECLI 551
2. Case C-210/16 Wirtschaftsakademie- Schleswig-Holstein [2018] ECLI 388

EU LAW

1. 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) [2016] OJ L 119
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Cass. Civ. 2, 2 April 1997, Bulletin II, no. 112/1997
2. Norway Act of 15 June 2018 no. 38 (Applicable Data Protection Law), LOV. 116/2018
3. Belgian Law of 30 July 2018 (Data Protection Acts), BELGISCH STAATSBLAD 05.09.2018, p. 68616.

WEBSITE REFERENCES

1. Advocate General, Michal Bobek, Opinions delivered in case Fashion ID, C-40/17, Retrieved from [http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&doclang=EN] Accessed 05.05.2019
2. Article 29 Working Party's Opinion 5/2009 on online social networking, adopted on 12 June 2009 (WP 163), retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf] Accessed 08.02.2019
3. Article 29. Working Party Opinion 1/2010 (adopted on 16 February 2010, reference number 00264/EN/WP 169) retrieved from [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] Accessed 08.02.2019
4. Detlev G.; Hickman T., *Obligations of controllers, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law*, 2019, retrieved from [https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection] Accessed 09.02.2019
5. Italian Data Protection Authority, *Titolare, responsabile, incaricato - Precisazioni sulla figura del 'titolare' - 9 dicembre 1997*, doc. web. n. 39785 Retrieved from [https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785] Accessed 20.02.2019
6. Niamh C. G. *et. al., GDPR: an impediment to research?*, Ir J Med Sci, 2019, Retrieved from [https://doi.org/10.1007/s11845-019-01980-2] Accessed 08.02.2019

7. Pereira Dias, A. G., *Portugese tort law: a comparison with the Principles of European Tort Law*, Conference Paper, 2004, p. 461, retrieved from [https://estudogeral.sib.uc.pt/bitstream/10316/2563/1/European_Principles_Tort_Law_Portugal.pdf] Accessed 10.05.2019
8. *What is a data controller or a data processor?* retrieved from [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en] Accessed 15.02.2019