Liability under EU Data Protection Law

From Directive 95/46 to the General Data Protection Regulation

by **Brendan Van Alsenoy***

Abstract: This article analyses the liability exposure of organisations involved in the processing of personal data under European data protection law. It contends that the liability model of EU data protection law is in line with the Principles of European Tort Law (PETL), provided one takes into account the "strict" nature of controller liability. After analysing the liability regime of Directive 95/46, the article proceeds to highlight the main changes brought about by the General Data Protection Regulation. Throughout the article, special consideration is given to the nature of the liability exposure of controllers and processors, the burden of proof incumbent upon data subjects, as well as the defences available to both controllers and processors.

Keywords: Data protection; controller; processor; Directive 95/46; General Data Protection Regulation; GDPR; Principles of European Tort Law; PETL; liability

Recommended citation: Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 (2016) JIPITEC 271 para 1.

A. Introduction

1 Practically every organisation in the world processes personal data. In fact, it is difficult to imagine a single organisation which does not collect or store information about individuals.[1] European data protection law imposes a series of requirements designed to protect individuals when their data are being processed.[2] European data protection law also distinguishes among different types of actors who may be involved in the processing. As far as liability is concerned, the most important distinction is the distinction between "controllers" and "processors". The controller is defined as the entity who alone, or jointly with others, "determines the purposes and means" of the processing.[3] A "processor", on the other hand, is defined as an entity who processes personal data "on behalf of" a controller.[4] Together, these concepts provide the very basis upon which

[1] Under EU data protection law, "personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject') [...]" (see art. 2(a) Directive 95/46; art. 4(1) GDPR). "Processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (art. 2(b) Directive 95/46; art. 4(2) GDPR).

[2] P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Claes, Duff and Gutwirth (eds.), *Privacy and the Criminal Law* (Intersentia, 2006), p. 76. See also R. Gellert, "Understanding data protection as risk regulation", *Journal of Internet Law* 2015, p. 3-16.

[3] Art. 2(d) Directive 95/46; art. 4(7) GDPR.

[4] Art. 2(e) Directive 95/46; art. 4(8) GDPR.

responsibility for compliance is allocated. As a result, both concepts play a decisive role in determining the liability exposure of an organisation under EU data protection law.[5]

2 For almost 15 years, Directive 95/46 stood strong as the central instrument of data protection regulation in the EU.[6] In 2010, however, the Commission announced that the time for revisions had come.[7] The Commission considered that while the objectives and principles underlying Directive 95/46 remained sound, revisions were necessary in order to meet the challenges of technological developments and globalisation.[8] A public consultation conducted in 2009, revealed concerns regarding the impact of new technologies, as well as a desire for a more comprehensive and coherent approach to data protection.[9] During the consultation, several stakeholders also raised concerns regarding the concepts of controller and processor.[10] Various solutions were put forward, ranging from minor revision to outright abolition of the concepts. In the end, the EU legislature opted to retain the existing concepts of controller and processor in the General Data Protection Regulation (GDPR).[11] Notable changes were made however, with regards to the allocation of responsibility and liability among the two types of actors.

3 The aim of this article is two-fold. First, it seeks to clarify the liability exposure of controllers and processors under EU data protection law. Second, it seeks to highlight the main differences between Directive 95/46 and the GDPR regarding liability allocation. The article begins by analysing the liability regime of Directive 95/46. The primary sources of analysis shall be the text of the Directive itself, its preparatory works, and the guidance issued by the Article 29 Working Party. Where appropriate, reference shall also be made to the preparatory works of national implementations of the Directive (e.g. the Netherlands, Belgium), as a means to supplement the insights offered by the primary sources. Last but not least, the Principles of European Tort Law (PETL), as well as national tort law, will be considered for issues not addressed explicitly by Directive 95/46.[12] The second part of this article will analyse the liability regime of the GDPR. Here too, the analysis shall be based primarily on the text of the GDPR itself, its preparatory works, and the Principles of European Tort Law.

B. Directive 95/46: a "strict" liability regime for controllers

4 Under Directive 95/46, a controller is, as a matter of principle, liable for any damages caused by the unlawful processing of personal data. Article 23(1) stipulates that Member States must provide that the controller shall be liable towards data subjects for any damages suffered as a result of an unlawful processing operation. A controller may be exempted from liability, however, in whole or in part, "if he proves that he is not responsible for the event giving rise to the damage" (article 23[2]). Directive 95/46 does not contain any provisions regarding the liability exposure of processors. While article 16 stipulates that processors may only process the data in accordance with the instructions of the controller, the Directive does not explicitly allocate liability in case of a disregard for instructions.

[5] Unfortunately, the distinction between controllers and processors is not always easy to apply in practice. For a more detailed discussion see B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *Computer Law & Security Review* 2012, Vol. 28, p. 25-43.

[6] The European Commission assessed its implementation in 2003 and 2007, both times concluding there was no need for revisions. See COM (2003) 265, "Report from the Commission - First Report on the implementation of the Data Protection Directive 95/46/EC)", at 7 and COM (2007)87, "Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive", p. 9.

[7] COM(2010) 609, "A comprehensive approach on personal data protection in the European Union", p. 2.

[8] *Ibid*, p. 3.

[9] COM(2010) 609, "A comprehensive approach on personal data protection in the European Union", p. 4.

[10] See e.g. Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data" (2009), p. 2-3; International Chamber of Commerce (ICC), ICC Commission on E-business, IT and Telecoms, "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data" (2009), p. 4; Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data" (2009), at paragraph 19 and European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework" (2009), p. 5.

[11] The definitions of controller and processor contained in the GDPR are quasi identical to the definitions contained in Directive 95/46. Only minor linguistic edits were made, none of which brought about a substantive change to the definitions.

[12] It should be noted that, as an academic piece, the PETL do not enjoy legal authority as such. Nevertheless, the PETL offer an interesting frame of reference when assessing any regulation of liability at European level, as they reflect what leading scholars have distilled as "common principles" for European tort law liability. For additional information see <http://www.egtl.org>.

I. Controller liability

1. Nature of controller obligations

5 To properly understand the liability exposure of controllers, it is necessary to first understand the nature of controller obligations. Directive 95/46 imposes a variety of obligations upon controllers. In certain instances, the obligations specify a *result* to be achieved (e.g., "personal data must be collected for legitimate purposes and not further processed in a way incompatible with those purposes").[13] In other instances, the obligations are specified as an obligation to make *reasonable efforts* to do something ("obligation of means"). For example, article 6(1)d provides that the controller must take "every reasonable step" to ensure that data which are inaccurate or incomplete shall be erased or rectified. Similarly, article 17(1) requires the controller to implement "appropriate" measures to ensure the confidentiality and security of processing. Finally, it should be noted that certain requirements necessitate a further assessment in light of the specific circumstances of the processing (e.g., whether or not personal data are "excessive" will depend inter alia on the purposes of the processing). The precise nature of the controller's obligations must therefore always be determined in light to the specific wording of each provision.

6 Article 23(1) provides that the controller shall be liable towards data subjects for any damages suffered "as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive". The liability rule of article 23 has been characterised as a form of "strict" (i.e. "no fault") liability.[14] The reason for this characterisation is the finding that the controller cannot escape liability simply by demonstrating the absence of a "personal fault". Likewise, it is not necessary for data subjects to demonstrate that the unlawful act was personally committed by the controller.[15] One should be careful however, to not overstate the "strict" nature of controller liability.[16] Even though the data subject is not required to demonstrate a "personal fault" on the part of the controller, he or she must in principle still succeed in proving the performance of an "unlawful act".[17] Demonstration of an "unlawful act" generally amounts to a demonstration of "fault" for tort law purposes.[18] Conversely, if the controller can establish that the processing complies with the requirements of the Directive, he will effectively exempt himself from liability on data protection grounds.[19] The characterisation of controller liability as "strict" liability (i.e. the notion that a controller may be still be held liable in absence of a personal fault) is therefore mainly relevant in relation to (1) controller obligations which impose an obligation of result; and (2) the liability of a controller for acts committed by his processor.

2. Non-delegable duty of care

7 Under Directive 95/46, the controller has a general duty to ensure compliance. Because the processor is seen as a "mere executor", who simply acts in accordance with the instructions issued by the controller, the Directive maintains that the responsibility for ensuring compliance remains with the controller. The mere fact that the unlawful action was performed by the processor rather than the controller does not diminish the controller's

[13] Art. 6(1)b Directive 95/46.

[14] Instruments of Parliament (Belgium), Memorie van Toelichting, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1990-1991, 6 May 1991, nr. 1610-1, p. 54 and D. De Bot, *Verwerking van persoonsgegevens* (Kluwer, 2001), p. 241. See also T. Léonard and Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution", *Journal des Tribunaux* 1999, p. 394 at nr. 65. Certain authors also refer to the "objective liability" of the controller. Although the terms "strict" and "objective" appear to be used interchangeably at times, some authors associate different legal consequences to the respective terms. For purposes of conceptual clarity, only the term "strict liability" shall be used in this article.

[15] Instruments of Parliament (Belgium), op. cit. supra note 14 and D. De Bot, op. cit. *supra* note 14.

[16] See also E. Reid, "Liability for Dangerous Activities: A Comparative Analysis", *The International and Comparative Law Quarterly* 1999, p. 736-737 (noting that strict liability is not always "stricter "than fault-based liability, particularly in cases where the circumstances giving rise to liability coincide in large measures with those used in negligence analysis) and E. Karner, "The Function of the Burden of Proof in Tort Law", in Koziol and Steininger (eds.), *European Tort Law 2008* (Springer, 2009), p. 76-77 (arguing that in practice "fault-based" liability and "strict" liability are not two clearly distinct categories of liability, but rather two extremes in a continuum, with many variations between them as regards the possibility of exculpation).

[17] See also *infra*; section B.I.3. See also Tweede Kamer der Staten-Generaal (Netherlands), Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *Vergaderjaar* 1997-1998, 25 892, nr. 3, p. 176.

[18] See art. 4:101 and 4:102(3) of the Principles of European Tort law (PETL): "A person is liable on the basis of fault for intentional or negligent violation of the required standard of conduct" and "Rules which prescribe or forbid certain conduct have to be considered when establishing the required standard of conduct.") See however also V. Ulfbeck and M.-L. Holle, "Tort Law and Burden of Proof – Comparative Aspects. A Special Case for Enterprise Liability?", in H. Koziol and B.C. Steininger (eds.), *European Tort Law 2008* (Springer, 2009), p. 35-36.

[19] See also Judgment of 19 June 2003, Kh. Kortrijk, 1st Ch. (Belgium), (2007) *Tijdschrift voor Gentse Rechtspraak*, p. 96.

liability exposure.[20] The controller shall in principle be liable for any violation of the Directive resulting from the operations carried out by a processor acting on its behalf ("as if they were performed by the controller"). In other words, Directive 95/46 imposes upon controllers a "non-delegable duty of care": the duty of care that a controller owes data subjects cannot be transferred to an independent contractor.[21]

8 A controller cannot escape liability for actions undertaken by its processors by demonstrating an absence of fault in either his choice or supervision of the processor.[22] This is a consequence of the strict liability imposed upon controllers: a controller can only escape liability by demonstrating that the processing complies with the requirements of the Directive or by proving an "event beyond his control" (article 23[2]).[23] The EU legislator chose to attach liability to the quality of a person as data controller (*qualitate qua*), without making any reference to possible exemptions other than the one mentioned in article 23(2).[24]

9 The liability of the controller for the actions performed by its processor is similar to the vicarious liability of a principal for the actions undertaken by its auxiliaries, whereby "a person is liable for damage caused by his auxiliaries acting within the scope of their functions provided that they violated the required standard of conduct".[25] In case of processors, however, the relationship with the controller in principle is not hierarchical in nature. While the processor is legally prohibited from processing the data "except on the instructions of the controller", he is not necessarily a "subordinate" of the controller.[26] As a result, the processor will in principle not be formally considered as an "auxiliary" of the controller for tort law purposes, although the outcome may be similar in practice.[27]

3. Burden of proof

10 To hold a controller liable, the data subject must succeed in demonstrating three elements: namely (1) the performance of an "unlawful act" (i.e. an unlawful processing operation or other act incompatible with the national provisions adopted pursuant to the Directive); (2) the existence of damages; and (3) a causal relationship between the unlawful act and the damages incurred.[28] In addition, the data subject

[20] See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17 and C. De Terwangne and J.-M. Van Gyseghem, "Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution", in C. De Terwangne (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, p. 125.

[21] Compare Reid, op. cit. *supra* note 16, p. 752-753 (explaining that a principal may be liable for the negligence of its contractors in cases where the law imposes a non-delegable duty of care). Liability for breach of non-delegable duty of care is not the same as vicarious liability, although the two can easily be confused. In case of vicarious liability, liability is "substitutional", whereas in case of a non-delegable duty of care, liability is personal (i.e. originates from a duty which is personal to the defendant). For a more detailed discussion see C. Witting, "Breach of the non-delegable duty: defending limited strict liability in tort", 2006 *University of New South Wales Law Journal*, p. 33-60.

[22] Contra: U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft, 1997), p. 264 (arguing that the intent of the European legislator was to exempt the controller not only in case of force majeure but also in cases where the controller had taken all the appropriate measures required by art. 17).

[23] Cf. *infra*; section B.I.4.

[24] The legislative history of 23(2) makes clear that the EU legislator intended to render the controller strictly liable for the actions committed by his processor by removing the reference to "suitable measures" (which had been present in both the initial and amended European Commission proposal) and by limiting the possible defense of the controller to "events beyond his control", such as force majeure. It stands to reason that the EU legislator thus deliberately chose to derogate from the general principle that a person shall not be liable for the actions performed by independent contractors. See also *infra*; note 38. Compare also with art. 7:102 of the Principles of European Tort Law (PETL) ("Strict liability can be excluded or reduced if the injury was caused by an unforeseeable and irresistible (a) force of nature (force majeure), or (b) conduct of a third party.").

[25] Art. 6:102 of the Principles of European Tort Law (PETL). See also C. von Bar a.o. (eds.) "Principles, Definitions and Model Rules of European Private Law - Draft Common Frame of Reference (DCFR)", Study Group on a European Civil Code and the Research Group on EC Private Law, 2009, p. 3318 et seq.

[26] Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 61. While art. 17(2) Directive suggests that the controller must supervise "the processor's implementation of organisational and security measures (by using the phrasing "and must ensure compliance with those measures"), the Directive does not bestow upon the controller a general power of instruction or supervision.

[27] Needless to say, in cases where the processor is a natural person, it may not be excluded that he or she might *de facto* operate in a hierarchical relationship with the controller, despite being labelled as an "independent contractor" in his or her contract with the employer. In cases where the person carrying out the services should legally be qualified as an "employee" rather than an "independent contractor", he or she will of course be treated as an "auxiliary" for tort law purposes.

[28] D. De Bot, "Art. 15bis Wet Persoonsgegevens", in X., *Personen- en familierecht. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer* (Kluwer, 2001), looseleaf. See also Raad van State (Belgium), Advies van de Raad van State bij het voorontwerp van wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij Verkeer van die gegevens, 2 February 1998, *Parl. St.* Kamer 1997-1998, nr. 1566/1, p. 145. See also U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 264. It should be noted that certain authors consider that it may be sufficient for the data subject

must also establish, as a preliminary matter, that the defendant is (or was) acting as the "controller" of the processing.[29]

11 The burden of proof incumbent upon data subjects can be quite onerous. First, identifying the controller of the processing at issue may be a complicated exercise, especially where more than one party is involved in the processing. Second, demonstrating the performance of an "unlawful act" may also be a challenge, particularly in cases where the Directive specifies an obligation of means (rather than an obligation of result), or requires further interpretation (e.g., an assessment of proportionality).[30] Demonstrating causality can also be difficult especially in cases where a particular outcome may be caused by different factors. For example, it may be difficult to prove that the unlawful collection of information (e.g., information regarding the ethnicity of a loan applicant) actually caused the damages to occur (e.g., the denial of a loan may be attributed to many different factors).[31] Finally, demonstrating recoverable damages (e.g., loss of reputation, emotional distress) can also be a challenge.[32]

12 A major difficulty for data subjects is that the evidence relevant to their case is often only accessible to the controller or its processor. Because personal data processing is generally conducted "behind closed doors", it can be difficult for data subjects to obtain solid evidence substantiating their claims.[33] Depending on the facts at hand however, the data subject may be able to invoke a *presumption* or other *judicial construct* with similar effect to help substantiate its claim. For example, in a case involving the unauthorised disclosure of personal data, the European Union Civil Service Tribunal has considered that the burden of proof incumbent upon the applicant may be relaxed:

> *"in cases where a harmful event may have been the result of a number of different causes and where the [defendant] has adduced no evidence enabling it to be established to which of those causes the event was imputable, although it was best placed to provide evidence in that respect, so that the uncertainty which remains must be construed against it".*[34]

13 The reasoning of the Civil Service Tribunal can be seen as an application of the so-called "proof-proximity principle", which allocates the evidential burden of proof on the party to whom the evidence is available, or whomever is better situated to furnish it easily and promptly.[35] Another judicial construct which may benefit certain data subjects is the adage of "*res ipsa loquitur*" ("*the thing speaks for itself*"), pursuant to which negligence may be inferred in cases where the harm would not ordinarily have occurred in the absence of negligence.[36] It should be

demonstrate the performance of an "unlawful act" and the existence of damages in order to hold the controller liable, without additionally requiring a demonstration of a causal relationship between the unlawful act and the damages suffered. See e.g. C. De Terwangne and J.-M. Van Gyseghem, "Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution", in C. De Terwangne (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, p. 125. In my view, this interpretation runs counter to the literal wording of article 23(1) of the Directive, which stipulates that the controller is obliged to indemnify the data subject for damages suffered "*as a result of*" an unlawful processing operation. As will be discussed later however, there exist certain judicial constructs through which the evidentiary burden of the data subject in this respect may be alleviated.

[29] See also C. von Bar a.o. (eds.) op. cit. *supra* note 25, p. 2994, at paragraph 31 ("The axiom [...], as far as tort law is concerned, is as far as tort law is concerned, is that the plaintiff must plead/establish and prove all of the requirements pertaining to his claim, in particular damage, grounds of liability and causation save where express regulations permit departures from this rule, whereas it is incumbent upon the defendant to show and prove certain requirements which give rise to a ground of defence, thereby displacing the claimant's assertions"). See also the Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161 and the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraph 141.

[30] T. Léonard and Y. Poullet, op. cit. *supra* note 14, 394 at nr. 65 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf.

[31] *Id.* De Bot indicates the doctrine of "loss of a chance" might be useful in this respect: see D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. For a comparative discussion of the "loss of a chance" doctrine see V. Ulfbeck and M.-L. Holle, op. cit. *supra* note 18, p. 40-43.

[32] See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report, Centre on Regulation in Europe, 25 January 2016, p. 58, available at <http://cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf> (last accessed 6 November 2016).

[33] P. De Hert, V. Papakonstantinou, D. Wright and S. Gutwirth, "The proposed Regulation and the construction of a principles-driven system for individual data protection", *The European Journal of Social Science Research* 2013, p. 141.

[34] Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161. See also the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraphs 141-142.

[35] C. Volpin, "The ball is in your court: Evidential burden of proof and the proof-proximity principle in EU competition law", *Common Market Law Review* 2014, p. 1173-1177. See also E. Karner, "The Function of the Burden of Proof in Tort Law", op. cit. *supra* note 16, p. 72-73.

[36] See V. Ulfbeck and M.-L. Holle, op. cit. supra note 18, p. 32-35; F.E. Heckel and F.V. Harper, "Effect of the doctrine of res ipsa loquitur", 22 *Illinois Law Review*, p. 724-725 and F. Dewallens and T. Vansweevelt, *Handboek gezondheidsrecht Volume I*, 2014, Intersentia, p. 1329. While the doctrine of *res ipsa loquitur* appears similar to reasoning of Civil Service Tribunal, there is a difference: the presumption of the Civil Service Tribunal pertained to the *attribution* of an act of negligence, whereas *res ipsa loquitur* concerns the *existence* of negligence. In case of *res ipsa loquitur* however, the requirement of attribution shall also be satisfied as one of the conditions for application of the doctrine is that the object which caused harm was under the exclusive control of the defendant *(Id.)*.

noted however, that the ability for the data subject to avail him- or herself of a particular presumption or construct, may vary according to the domestic legal system of each Member State.

4. Defences

14 Article 23(2) stipulates that "the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage". The question inevitably arises as to the nature of the evidentiary burden of proof incumbent upon controllers. Which evidence must controllers offer to successfully exempt themselves from liability, either for their own actions or for the actions performed by their processors or auxiliaries?

15 In order to prove that he is "not responsible for the event giving rise to the damage", the controller must demonstrate three things: (1) the occurrence of an event; (2) which caused the damage; and (3) which cannot be attributed to the controller.[37] In principle, mere demonstration of an absence of fault on the part of the controller is not sufficient.[38] Once it is established that the damage was caused by an unlawful processing operation, the controller can only escape liability by demonstrating that the damages occurred only as the result of an event that cannot be attributed to him.[39]

16 The wording "not responsible for the event giving rise to the damage" recalls the concept of an "external cause" or "event beyond control", which in many jurisdictions is accepted either (1) as a justification ground excluding fault, or (2) as a means to demonstrate the absence of a causal relationship.[40] According to the Draft Common Frame of Reference, an event beyond control is "an abnormal occurrence which cannot be averted by any reasonable measure" and which does not constitute the realisation of a risk for which the person is strictly liable.[41] The aim of the liability exemption is therefore not to reduce the "strict" liability of the controller. Rather, its aim is to keep the strict liability within the borders of the risk for which it exists.[42] Recital (55) provides two examples of events for which the controller cannot be held responsible: namely, (1) an error on the part of the data subject;[43] and (2) a case of force majeure.[4445]

[37] This point was emphasized by the Belgian Council of State during its evaluation of the bill implementing Directive 95/46. See Raad van State (Belgium), op. cit. *supra* note 28, p. 145.

[38] *Ibid*, p. 146. During the legislative history of Directive 95/46, the escape clause of art. 23(2) underwent several revisions. In the initial Commission proposal, the escape clause provided that the controller of the file would not be liable for damages resulting from the loss or destruction of data or from unauthorized access if he could prove that he had taken "appropriate measures" to comply with requirements of art. 18 and 22 (security and due diligence). (COM(90) 314, "Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security", p. 40.) The European Parliament amended the text to state that the controller must compensate the data subject for any damage "resulting from storage of his personal data that is incompatible with this directive." (O.J. 1992, C 94/192, "Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992" (First Reading), p. 192. The Parliament's proposed change had the effect of removing the escape clause contained in the initial Commission proposal. The European Commission felt strongly however, that the Member States should be able to exempt controllers from liability, if only in part, for damage resulting from the loss or destruction of data or from unauthorized access "if he proves that he has taken suitable steps to satisfy the requirements of Art. 17 and 24." (O.J. 1992, C 311/54, COM (92) 422, "Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", p. 54. In the end, the issue was settled by the Council, which drafted the final version of 23(2), which provides that: "The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage." The Council clarified the meaning of art. 23(2) by way of a recital which stipulated that "[...] whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he reports an error on the part of the data subject or in a case of force majeure".

[39] See in the same vein also M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", (2015) *University of Hong Kong Faculty of Law Research Paper*, No. 2015/45, p. 23-24 (noting that the language of art. 23(2) does not concern itself with the imputation of fault or culpability to the controller, but with the imputation of the facts themselves).

[40] See C. von Bar a.o., op. cit. *supra* note 25, p. 3538 et seq. and art. 7:102 of the Principles of European Tort Law (PETL) (defences against strict liability).

[41] *Id.*

[42] C. von Bar a.o., op. cit. *supra* note 25, p. 3539.

[43] The reference to "an error on the part of the data subject" recalls the concept of "contributory negligence" or "contributory fault", whereby a victim whose own faulty behaviour has contributed to the occurrence of his own damage, is not entitled to compensation to the extent that his behaviour contributed to the damage. See von Bar a.o., op. cit. *supra* note 25, p. 3475-3500 and p. 3539. See also H. Cousy and D. Droshout, "Fault under Belgian Law", in P. Widmer (ed.), *Unification of Tort Law: Fault*, Kluwer Law International, 2005, p. 36.

[44] "*Force majeure*" or "*Act of God*" can be described as an unforeseeable and unavoidable event which occurs independent of a person's will. For a discussion of the specific requirements for *force majeure* in different Member States see C. von Bar a.o., op. cit. *supra* note 25, p. 3540 et seq.

[45] According to the parliamentary works relating to the implementation of Directive 95/46 into Belgian law, other events which cannot be attributed to the controller can

17 Article 23(2) of Directive 95/46 provides the only valid defence for controllers once the data subject has satisfied its burden of proof. In practice, controllers will not wait until the burden of proof shifts to them. Most controllers will try to ward off liability by arguing that the conditions of liability are simply not met, e.g. by demonstrating the absence of illegality in the processing. Again, the nature of the controller obligation at issue will be determinative here. Where an obligation of means is concerned, controllers can effectively avoid liability by demonstrating that they implemented every reasonable measure that might be expected of them. Even where an obligation of result is involved, controllers may seek to avoid liability by reference to the *Google Spain* ruling, where the Court of Justice indicated that there may also be practical considerations which limit the responsibilities of controllers.[46] In particular, when qualifying search engine providers as "controllers", the Court of Justice indicated that there may be practical limits to the scope their obligations:

> *"[...] the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 [...]".*[47]

18 By explicitly referring to the "powers and capabilities" of the search engine operator, the Court of Justice implicitly acknowledged that there may be practical limits to the ability of a search engine operator to meet all the obligations resulting from Directive 95/46.[48] In particular, it can be argued that *Google Spain* does not oblige search engine providers to exercise preventative control over the information it refers to.[49] In fact, the reasoning of the Court of Justice suggests that the obligations of search engine providers concerning third-party data is essentially only "reactive"; only after the provider has been made aware of the fact that the display of specific search results following a name search adversely impacts the data subject, must the provider assess whether or not delisting is necessary.[50]

5. Eligible damages

19 In principle, there is no restriction as to the type or amount of damages that data subjects may claim. Data subjects can claim both material (e.g., loss of a chance) and non-material damages (e.g. loss of reputation, distress).[51] Of course, the general rules on damages shall also apply here (e.g. personal interest, actual loss, etc.).[52]

II. Processor liability

20 Directive 95/46 does not contain any provision regulating the liability of processors. It also does not impose any obligations directly upon processors, with one exception: article 16 of Directive 95/46 requires the processor not to process personal data "except on the instructions from the controller". While Directive 95/46 does foresee additional obligations for processors, it envisages them as being

also be considered as a possible defence (e.g., the act of a third party for which the controller is not accountable). See Instruments of Parliament (Belgium), op. cit. *supra* note 14, p. 54 and D. De Bot, *Verwerking van persoonsgegevens*, op. cit. supra note 14, p. 241. Of course, the presence of a justification ground does not suspend the general duties of care of a controller. If the controller could have foreseen the damages and prevent them by taking anticipatory measures, normal rules of negligence apply. See also C. von Bar a.o., op. cit. *supra* note 25, p. 3538.

[46] See also H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", *Maastricht Journal of European and Comparative Law* 2014, p. 55 and Article 29 Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" (2014), WP 225, p. 6) ("The ruling does not oblige search engines to permanently carry out that assessment in relation to all the information they process, but only when they have to respond to data subjects' requests for the exercise of their rights."). These considerations are particularly relevant as regards the general prohibition to process certain "sensitive" categories of data, which is in principle formulated as an obligation of result.

[47] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 38, emphasis added.

[48] For a more narrow reading see M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *supra* note 39, p. 26.

[49] See also H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", Maastricht Journal of European and Comparative Law 2014, p. 559 ("For me, it is obvious that this judgment does not mean that a search engine provider should exercise preventive control over the information it disseminates, nor that it is in any other manner limited in its essential role of ensuring a free internet. In essence, the Court confirms that a search engine – which has as its core activity the processing of large amounts of data with potentially important consequences for the private life of individuals –cannot escape from responsibility for its activities.").

[50] See also Article 29 Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" (2014), WP 225, p. 6).

[51] U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 263 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. See also Court of Appeal (Civil Division), *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311 (27 March 2015), at paragraphs 70-79.

[52] For a discussion of the general rules of damages under Belgian law see e.g. S. Stijns, *Verbintenissenrecht*, Boek 1bis, Die Keure, 2013, 101-104.

of a contractual nature. In particular, article 17(3) of Directive 95/46 provides that when a controller engages a processor to carry out certain processing operations on his behalf, their relationship must be governed by a contract or other legal act "binding the processor to the controller", which must specify that the processor is obliged (1) to follow the controller's instructions at all times, and (2) to implement appropriate technical and organisational measures to ensure the security of processing.[53] Article 17(3) mentions only the minimum content that should be included in an arrangement between controllers and processors. According to the Working Party, the contract or other legal act should additionally include "a detailed enough description of the mandate of the processor".[54]

21 The absence of a clear liability model for processors under Directive 95/46 begs the question of whether processors may be held liable by data subjects. In answering this question, a distinction should be made between two scenarios. In the first scenario (scenario A), the processor merely fails to give effect to the instructions issued by the controller (e.g., fails to implement the security measures instructed by the controller or fails to update information as instructed by the controller). In the second scenario (scenario B), the processor decides to process personal data for his own purpose(s), beyond the instructions received by the controller (in other words, to act outside the scope of his "processing mandate").

1. Scenario A: processor fails to implement controller instructions

22 In scenario A, the data subject shall in principle only be able to hold the processor liable on the basis of data protection law if this is provided by the national legislation implementing Directive 95/46.[55] Article 49(3) of the Dutch Data Protection Act, for example, provides that the processor can be held liable by data subjects insofar as the damages resulted from his activities.[56] In contrast, the Belgian Data Protection Act does not recognise a right for data subjects to hold processors liable as such. A data subject might nevertheless be able to hold a processor liable if he can demonstrate that the actions of the processor constituted "negligence" or violated another legal provision.[57] The standard of care incumbent upon the processor may, however, be informed by the contract between controller and processor.[58] In any event, the controller who has been held liable by the data subject, should be able to claim back the damages from the processor on the basis of the contract between them.[59]

2. Scenario B: processor acts outside of processing mandate

23 In scenario B, the processor does not merely fail to observe the instructions issued by the controller,

[53] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'" (2010), WP 169, p. 26.

[54] *Id.* See also U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 232 (noting that the contract or legal act should generally address all data protection issues including, for example, how to deal with access requests by governments or other interested third parties). In practice, the legal act binding the processor to the controller shall most often take the form of a contract. The reference to "other" legal acts in art. 17(3) mainly concerns the public sector, where a processor might be appointed either directly by way of legislation or by way of a unilateral decision of a public body. (U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 231).

[55] See also Article 29 Data Protection Working Party, op. cit. supra note 53, p. 28. ("*[W]hile the Directive imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, also the processor should be considered liable in certain cases.*").

[56] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Staatsblad* 302 (Netherlands). See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 62 and p. 176. Another example of a national law which imposes liability directly upon processors is the Czech Data Protection Act (see art. 8 of Act No. 101/2000 Coll., on the Protection of Personal Data, 4 April 2000, English version accessible at <https://www.uoou.cz/en>).

[57] D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. Generally speaking, it will be more appealing for the data subject to seek damages from the controller, because (a) the identity of the processor may not be known to the data subject (b) it will generally be more difficult for data subject to establish a violation of general duty of care by processor.

[58] See e.g. A. De Boeck, "Aansprakelijkheid voor gebrekkige dienstverlening", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid* (Kluwer, 2008), II.3-84o-p. See also S. Demeyere, I. Samoy and S. Stijns, *Aansprakelijkheid van een contractant jegens derden – De rechtspositie van de nauw betrokken derde*, Die Keure, 2015, p. 37 et seq. The standard of care incumbent upon processor may in principle also be assessed in light of the professional occupation and knowledge of the processor: see e.g. H. Cousy and D. Droshout, "Fault under Belgian Law", op. cit. *supra* note 43, p. 32 and p. 39. In Belgium, plaintiffs may also need to consider the so-called "*rule of the (quasi-)immunity of the contractor's agent*" in cases where there is a contractual relationship between the controller and the data subject. This rule may further limit the data subject's ability to seek redress directly from the processor. If the action by the processor amounts to a crime however, such limitations will not apply. For more information see H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", in J. Spier (ed.), *Unification of Tort Law: Liability for Damage Caused by Others*, Kluwer law International, 2003, p. 50; S. Stijns, op. cit. *supra* note 52, p. 143 et seq.

[59] See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 176.

but also decides to process the personal data for his own purposes. In such instances, the processor shall be considered to be acting as a controller in his own right, by virtue of determining his own "purposes and means" of the processing.[60] As a result, the (former) processor can be held liable in any event on the basis of national legislation implementing article 23 of Directive 95/46.[61] In principle, data subjects may also turn to the initial controller (who had entrusted the data to the (former) processor) for compensation. This is a result of the strict liability regime of article 23. The initial controller cannot escape liability by demonstrating an absence of fault in either his choice or supervision of the processor.[62] In practice, this means that the data subject will typically have the choice whether or not to sue both parties and whether or not to do so simultaneously or consecutively (although national tort law may specify otherwise).[63] Again, the initial controller should be able to claim back the awarded damages from the processor for disregarding his instructions on the basis of the contract between them.[64]

III. Multiple controllers

24 Not every collaboration among actors involving the processing of personal data implies the existence of a controller-processor relationship. It is equally possible that each actor processes personal data for its own distinct purposes, in which case each entity is likely to be considered a controller independently of the other ("separate controllers"). It is also possible that the actors jointly exercise decision-making power concerning the purposes and means of the processing, in which case they are considered to act as "joint controllers" or "co-controllers".[65]

1. Separate controllers

25 Separate controllers exchange personal data with one another, but do so without making any joint decisions about the purposes and means of any specific processing operation.[66] In such cases, each party is independently (yet fully) responsible for ensuring compliance of its own processing activities. In principle, the liability exposure of each party is also strictly limited to the processing activities under its own control. In exceptional cases however, liability may nevertheless be shared, particularly where failure to ensure compliance by one controller contributes to the same damages caused by the fault by another controller.

26 In the case of separate controllers, the starting point is that each controller is only responsible for ensuring compliance with its own activities ("*separate control, separate responsibilities*"). As Olsen and Mahler put it:

> *"In this type of multiple data controller relationship, the data controllers separately process personal data, but there is a data flow from one controller to the other. Each controller is responsible for his own processing, and the communication of personal data to the other data controllers is one example of such processing. One controller is not responsible for acts or omissions of the other data controller."*[67]

27 Because each controller is separately responsible for his own processing activities, only one controller shall in principle be liable in case of an unlawful processing operation (scenario A).[68] Liability may nevertheless be shared, however, if the fault of one controller brings about the *same damage* as the fault

[60] See also Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 25. A (former) processor shall be (re) qualified as a (co-)controller where he acquires a relevant role in determining either the purpose(s) and/or the essential means of the processing (Id.). See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 62.

[61] In principle, the processor may also be held liable on the basis of the national provision implementing art. 16 of Directive 95/46, which specifies that the processor may not process personal data "*except on the instructions of the controller*", which is a requirement directly applicable to processors. Depending on the jurisdiction, a breach of confidentiality by processors may also amount to a crime: see e.g. art. 38 of the Belgian Data Protection Act.

[62] This outcome is similar to the liability of principals for torts committed by their auxiliaries "*in the course of the service*" for which they have been enlisted (although results may vary depending on national tort law). See e.g. T. Vansweevelt and B. Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, 2009, Intersentia, p. 416-421 and H. Vandenberghe, "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, p. 604-606.

[63] In Belgium, victims of concurrent faults may hold both the tortfeasor and the vicariously liable party liable *in solidum*. See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 33-35. See also art. 9:101 PETL.

[64] See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 176.

[65] See also B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", op. cit. *supra* note 5, 34 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", (2007) *Computer, Law & Security Review*, p. 419.

[66] Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 19 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", op. cit. *supra* note 65, p. 419.

[67] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", Legal IST project, 2005, p. 41.

[68] Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

of another controller (scenario B).

a.) Scenario A

28 A hospital routinely shares information about a patient's treatments with an insurance company in order to obtain payment for the expenses relating to the patient's care. The sharing of personal information takes place with the explicit consent of the data subject and/or pursuant to national legislation. One day, the insurance company suffers a data breach as a result of insufficient security measures. Information about the patient's medical treatment is exposed, leading to considerable emotional harm. In principle, the patient will only be able to obtain compensation from the insurance company for the damages suffered because the hospital is not the controller of the processing operations undertaken by the insurance company.

b.) Scenario B

29 One day a hospital mistakenly transmits information about a patient's treatment to the wrong insurance company. The next day, that same insurance company suffers a data breach as a result of inadequate security measures. In such cases, the patient may be able to obtain compensation from both the hospital and the insurance company for the damages suffered as they each committed a fault contributing to the same damage.

30 Scenario B offers an example of *concurring faults*, whereby several distinct faults may be considered to have caused the same legally relevant damage.[69] What precisely constitutes "*the same damage*" is open to interpretation.[70] In certain jurisdictions, concurring faults lead either to solidary liability or liability *in solidum*.[71] If that is the case, each "concurrent tortfeasor" shall be obliged to indemnify the victim for the entire damage, irrespective of the severity of the fault leading to its liability.[72] The internal allocation of liability between the concurrent tortfeasors may nevertheless take into account the extent or severity of the fault.[73] In the case of scenario B, it would mean that the hospital would be obliged to indemnify the patient for the whole of the damages suffered, even though the hospital was not responsible as a controller for the poor security measures employed by the insurance company.

2. Joint controllers

31 In the case of joint control, several parties jointly determine the purposes and means of one or more processing activities. The distinction between "joint" and "separate" control may be difficult to draw in practice. The decisive factor is whether or not the different parties *jointly* determine the purposes and means of the processing at issue.[74] If the parties do not pursue the *same objectives* ("purpose"), or do not rely upon the *same means* for achieving their respective objectives, their relationship is likely to be one of "separate controllers" rather than "joint controllers". Conversely, if the actors in question do determine the purposes and means of a set of processing operations together, they will be considered to act as "joint controllers" or "co-controllers".[75]

[69] See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 29-35; S. Stijns, op. cit. *supra* note 52, p. 110-111 and T. Vansweevelt and B. Weyts, op. cit. *supra* note 62, p. 835-839.

[70] *Ibid*, p. 44-45 and S. Guiliams, "Eenzelfde schade of andere schade bij pluraliteit van aansprakelijken", *Nieuw Juridisch Weekblad* (NJW) 2010, afl. 230, p. 699-700 (arguing that different faults will be considered to have contributed to "the same damage" *if it is practically impossible to distinguish* to what extent the damage is attributable to each of the concurring faults).

[71] See C. von Bar a.o., op. cit. *supra* note 25, p. 3599 et seq. See also art. 9:101 of the Principles of European Tort Law (PETL).

[72] *Id.* The difference between solidary liability and *in solidum* liability is minimal: in both cases, the injured party is able to sue each of the debtors for relief of the whole amount. For more information see H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 29-36.

[73] *Id.* In Belgium, the apportionment of liability among the concurrent tortfeasors must in principle be based on the extent to which each concurring fault may be said to have caused the damage, rather than the severity of the fault. (S. Stijns, op. cit. *supra* note 52, 111 and S. Guiliams, "De verdeling van de schadelast bij samenloop van een opzettelijke en een onopzettelijke fout", *Rechtskundig Weekblad* (R.W.) 2010, p. 475.

[74] Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 19 ("*joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller*").

[75] Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 25. The distinction between joint and separate control was rendered more explicit in the 1984 UK Data Protection Act, which defined a data user as the person that "either alone or jointly or in common with other persons" controls the contents and use of the data (Section 1(5) of the 1984 Data Protection Act). As clarified by the Data Protection Registrar: "The control does not need to be exclusive to one data user. Control may be shared with others. It may be shared jointly or in common. 'Jointly' covers the situation where control is exercised by acting together. Control 'in common' is where each shares a pool of information, changing, adding to or using the information for his own purposes independently of the other". (The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Office of the Data Protection Registrar, 1989, p. 10-11.) See also the Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and

32 Directive 95/46 EC is essentially silent on how responsibility and liability should be allocated in case of joint control. The only guidance that can be found in the legislative history of Directive 95/46 is the following statement made by the European Commission:

> *"each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed".* [76]

33 The cited passage suggests that each co-controller is individually responsible for ensuring compliance of the processing as a whole and should therefore in principle be liable for any damages resulting from non-compliance ("*joint control, joint responsibilities*"). The liability among joint controllers shall in principle be solidary in nature (i.e. the harmed data subject may bring a claim against any of them for the entire amount of the damage).[77] Of course, the solidary liability of joint controllers only extends to those processing activities for which they in fact exercise joint control. In case of "partial joint control" (whereby certain processing operations are performed under the sole control of one controller),[78] responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.[79]

34 The solidary liability of joint controllers can be justified on the basis of the "common fault" committed by each controller. A "common fault" arises when multiple parties knowingly and willingly contribute to the same circumstance or event giving rise to the damage.[80] Common faults typically induce solidary liability.[81]

35 If the data subject decides to address only one of the joint controllers for the damages, that controller should be able to obtain redress from his fellow joint controllers for their contribution to the damages.[82] In principle, nothing prevents joint controllers from deciding how to allocate responsibility and liability among each other (e.g., by way of a joint controller contract).[83] The terms of such arrangements shall generally not however be opposable to data subjects, based on the principle of solidary liability for common faults.[84]

36 It should be noted that the Article 29 Working Party has defended an alternative point of view. Specifically, it has argued that joint control should not necessarily entail solidary ("joint and several") liability.[85] Instead, joint and several liability:

> *"should only be considered as a means of eliminating uncertainties, and therefore assumed only insofar as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances".*[86]

37 The approach of the Article 29 Working Party seems fair when it comes to the internal allocation of liability among joint controllers, but may potentially be unjust towards the harmed data subject. The approach suggests that a contract between joint controllers may be opposable to data subjects, and that a harmed data subject may carry the burden of deciding which of the joint controllers is "ultimately" responsible for the damages suffered. In my opinion, the viewpoint of the Article 29 Working Party does not find sufficient support in either the text or legislative history of Directive 95/46. In cases where joint control exists, each joint controller should in principle incur solidary liability for damages resulting from the "common" processing. Any arrangements between joint controllers, including those regarding liability, should not be opposable

computer bureaux", Data Protection Registrar, 1985, p. 12.

[76] COM (95) 375 final- COD287, "Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", p. 3. See also Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 17-18.

[77] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 46-48. See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

[78] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", op. cit. *supra* note 65, p. 420.

[79] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 46-48.

[80] See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 30; T. Vansweevelt and B. Weyts, op. cit. *supra* note 62, p. 839.

[81] See art. 9:101 of the Principles of European Tort Law (PETL). See also C. von Bar a.o., op. cit. *supra* note 25, p. 3599 et seq. and E. Karner, "The Function of the Burden of Proof in Tort Law", op. cit. *supra* note 16, p. 74.

[82] See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

[83] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 48.

[84] See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

[85] Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 22. In this context, the term "solidary liability" is synonymous with the term "joint and several liability".

[86] *Ibid*, p. 24.

to data subjects, based on the principle of solidary liability for common faults.[87]

C. The GDPR: a "cumulative" liability regime for controllers and processors

38 The GDPR has introduced several changes to the allocation of responsibility and liability among controllers and processors. While the controller is still the party who carries primary responsibility for compliance, processors have become subject to a host of obligations and are directly liable towards data subjects in case of non-compliance (article 82[2]). In situations involving more than one controller or processor, every controller or processor involved in the processing may in principle be held liable for the entire damage, provided the damage results from its failure to comply with an obligation to which it is subject (article 82[4]). The result is a "cumulative" liability regime, whereby each actor can be held liable in light of its role in the processing.

I. Controller liability

39 The liability model for controllers under the GDPR is essentially the same as under Directive 95/46. Article 82(2) of the GDPR provides that "[a]ny controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation." In other words, the controller remains generally liable for any damages arising from the unlawful processing personal data. The controller may be exempted from liability, in whole or in part, "if it proves that it is not in any way responsible for the event giving rise to the damage" (article 82[3]).

1. Nature of controller obligations

40 As under Directive 95/46, the actual liability exposure of controllers depends on the nature of the obligation in question. Many controller obligations under the GDPR are formulated as an obligation of means. For example, article 17(2) of the GDPR requires controllers who are obliged to erase data pursuant to the right to erasure, to take "reasonable steps" to inform other controllers that the data subject has requested the erasure. Moreover, it is worth noting that many controller obligations make reference to the notion of "risk" (e.g., data protection by design (article 25(1) GDPR), implying that the evaluation of risk may be a determinative factor in liability disputes. Only few controller obligations contained in the GDPR can be qualified as obligations of result. An interesting example is provided by article 13(3) of the GDPR, which concerns the duty to provide information to the data subject in case a controller who collected information from the data subject intends to further process data for a purpose other than that for which the data were collected.[88]

2. Non-delegable duty of care

41 The liability regime for controllers has remained "strict" under the GDPR: once an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault.[89] The controller shall therefore remain liable for unlawful processing activities undertaken by the processor on its behalf, even if the controller were to demonstrate an absence of fault in either his choice or supervision of the processor. Under the GDPR, a controller may in principle be exempted from liability (in whole or in part) in only two situations: (1) if the controller can prove it is not in any way responsible for the event giving rise to the damage (article 82[3]); and (2) if the controller satisfies the conditions for liability exemption for intermediary service providers contained in Directive 2000/31 (article 2[4]).[90]

3. Burden of proof

42 According to article 5(2) of the GDPR, controllers are under a general obligation to be able to demonstrate their compliance with the basic principles of data protection ("accountability"). Moreover, a number of other provisions additionally stipulate that the controller must be able to demonstrate compliance, such as the provisions regarding the conditions for consent (article 7), processing which does not allow identification (articles 11 and 12[2]), and the general obligation to adopt appropriate technical and organisational measures to ensure compliance (article 24).

43 Strictly speaking, the requirement that the controller should "be able" to demonstrate compliance does

[87] Again: in cases of partial joint control, responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.

[88] Interestingly, only in the situation where the personal data have been collected from the data subject is the duty to inform defined as an obligation of result. If the date have been obtained elsewhere, art. 14(5)a GDPR provides an exemption in case of disproportionate effort.

[89] Compare *supra*; section B.I.2.

[90] See also *infra*; section C.I.4.

not alter the burden of proof incumbent upon data subjects. After all, requiring the *ability* to demonstrate is not the same as requiring *actual* demonstration.[91] Such a formalistic reading would, however, run contrary to the principle of accountability which the GDPR seeks to promote.[92] The EU legislature did not introduce these provisions merely to promote better organisational practices, but also to require controllers to stand ready to demonstrate compliance when called upon to do so. As a result, one could argue that the data subject no longer carries the burden of proof of demonstrating exactly where the processing went wrong.[93] At the very least, the argument can be made that the provisions of the GDPR regarding accountability (which require controllers to "be able to demonstrate compliance") reinforce the notion that the controller is in fact "best placed" to proffer evidence of the measures it has taken to ensure compliance. Even if the legal burden of proof is still borne by the data subject, the evidential burden of proof should *de facto* shift to the controller as soon as the data subject has offered *prima facie* evidence of an unlawful processing activity.[94]

4. Defences

44 Article 82(3) GDPR provides that a controller or processor shall be exempt from liability if it proves that it is "not in any way" responsible for the event giving rise to the damage. Article 82(3) GDPR clearly echoes the escape clause of article 23(2) of Directive 95/46.[95] Interestingly, the GDPR does not contain a recital similar to recital (55) of Directive 95/46, which provides two examples of how a controller might prove that it is "not responsible for the event giving rise to the damage" (i.e., force majeure or error on the part of the data subject). Nevertheless, it is reasonable to assume that the words "not responsible for the event giving rise to the damage" should still be interpreted in the same way. As a result, the escape clause of article 82(3) still refers exclusively to "events beyond control", i.e. an abnormal occurrence which cannot be averted by any reasonable measures and which does not constitute the realisation of the risk for which the person is strictly liable.[96] If anything, the addition of the words "in any way" (in comparison to article 23[2] of Directive 95/46), suggests a desire to tighten the scope of the escape clause even further.[97]

45 A more significant development has been the formal recognition of the liability exemptions for internet intermediaries contained in the E-Commerce Directive. Article 2(4) GDPR specifies that the Regulation "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive". The clarification provided by article 2(4) GDPR is most welcome, given the uncertain status of these liability exemptions under Directive 95/46. Article 1(5)b of the E-Commerce Directive provides that it does not apply to "questions relating to information society services covered by Directive 95/46 [...]". A literal reading would suggest that the liability exemptions provided in the E-Commerce Directive should not be applied in cases concerning the liability of "controllers", as this is a matter regulated by Directive 95/46.[98]

46 The practical importance of article 2(4) of the GDPR should not be overstated. A reasonable interpretation of controller obligations shall generally not result in the imposition of liability in absence of both knowledge and control. The decision of the Court of Justice in *Google Spain*[99], as well as the decision of the Italian Supreme Court in *Google Video*[100],

[91] Only in art. 21 (right to object) does the GDPR specify that it is up to the controller to actually demonstrate the legality of his processing activities.

[92] For a detailed discussion regarding the origin and development of the principle of accountability see J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, 2012, Palgrave Macmillan, p. 49-82.

[93] See also P. De Hert, V. Papakonstantinou, D. Wright and S. Gutwirth, op. cit. *supra* note 33, p. 141.

[94] Regarding the distinction between *legal* burden of proof and the *evidential* burden of proof see C. Volpin, "The ball is in your court: Evidential burden of proof and the proof-proximity principle in EU competition law", *Common Market Law Review* 2014, p. 1177-1179.

[95] Cf. *supra*; section B.I.4.

[96] Cf. *supra*; section B.I.4.

[97] See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report", 2016, Centre on Regulation in Europe, p. 58.

[98] It should be noted, however, that even in relation to Directive 95/46 certain scholars have argued that controllers should in principle be able to benefit from the liability exemptions contained in the E-Commerce Directive, including in situations where the dispute concerns the unlawful processing of personal data. See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *International Data Privacy Law* 2013, p. 5 et seq.; G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law* 2014, p. 573 et seq. and M. de Azevedo Cunha, L. Marin and G. Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2012, p. 57-58.

[99] Cf. *supra*; section B.I.4.

[100] Sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, Corte di Cassazione, sez. III Penale, n. 5107/14, at paragraph 7.2 ("[...] as long as the offense is unknown to the service provider, it cannot be regarded as the controller of the processing, because it lacks any decision-making power on

clearly support this proposition. Nevertheless, the incorporation of the liability exemptions for internet intermediaries is likely to yield certain benefits. First, it should further the development of a more horizontal and uniform approach to the issue of intermediary liability.[101] In addition, article 15 of the E-Commerce Directive clearly provides that Member States may not impose general monitoring obligations upon internet intermediaries. While most would agree that internet intermediaries should not be expected to proactively monitor whether the personal data disseminated through their platform is being processed lawfully, the formal applicability of article 15 of Directive 2000/31 would offer certain providers greater legal certainty. But article 2(4) of the GDPR is by no means a panacea: the concepts of "hosting, "mere conduit", and "caching" contained in Directive 2000/31 are subjects of continuous debate and have themselves given rise to a fair degree of legal uncertainty.[102] Moreover, the liability exemptions of Directive 2000/31 would only affect the liability exposure of controllers in relation to mere distribution or storage activities. An absence of liability for mere distribution or storage does not however, imply an absence of responsibility with regard to other operations performed on that content. Many service providers perform additional operations which go beyond a purely "intermediary", "passive", or "neutral" capacity.[103] As a result, it may still be necessary to interpret the obligations of internet intermediaries as controllers in light of their "responsibilities, powers and capabilities", as suggested by the Court of Justice in *Google Spain*.[104]

5. Eligible damages

47 Article 82(1) GDPR explicitly recognises that data subjects may seek compensation for both material and non-material damages. The EU legislature has thereby clarified that the right to compensation extends to "non-pecuniary damages". While this was arguably already the case under Directive 95/46, the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU Member States.

II. Processor liability

48 In contrast to Directive 95/46, the GDPR imposes a range of obligations directly upon processors and renders them liable towards data subjects in the case of non-compliance (article 82[2]).

1. Nature of processor obligations

49 As is the case for controller liability, the liability exposure of processors depends on the nature of the obligation concerned. Many obligations incumbent upon processors are formulated as obligations of means rather than as obligations of result. For example, the obligation to secure the processing of personal data (article 32) is clearly an obligation of means. On the other hand, the obligation not to process personal data except on the instructions of the controller (article 29), has been formulated as an obligation of result. The precise nature of a processor's liability exposure must therefore also be determined in light of the specific wording of each obligation.

50 It should be noted that the GDPR has added considerable detail as regards to the legal binding of processors towards controllers (article 28[3]). Processors must comply not only with requirements that are directly applicable, but also with requirements imposed by way of contract. For example, article 28(3) foresees that the contract or other legal act between the controller and processor shall stipulate that the processor shall assist the controller in the fulfilment of its obligation to respond to requests for exercising the data subject's rights - insofar as this is possible and taking into account the nature of the processing.

51 Other obligations that are directly relevant to processors are the obligation to maintain a record of processing activities (article 30[2]), the obligation to notify data breaches to the controller (article 33[2]), the obligation to appoint a data protection officer (article 37), the adherence to codes of conduct and requirements of certification (articles 41 and 42), and restrictions regarding international transfers (article 44 et seq.).

the data itself, and when, instead, the provider is aware of the illegal data and is not active for its immediate removal or makes it inaccessible, however, it takes a full qualification of the data controller".) A special word of thanks is owed to Professor Giovanni Sartor for assisting me with this translation.

[101] M. de Azevedo Cunha, L. Marin and G. Sartor, op. cit. *supra* note 98, p. 57-58.

[102] See e.g. P. Van Eecke, "Online service providers and liability: a plea for a balanced approach", *Common Market Law Review* 2011, 1481 et seq.; E. Montéro, "Les responsabilités liées au web 2.0", *Revue du Droit des Technologies de l'Information* 2008, p. 364 et seq. and B. Van der Sloot, "Welcome to the Jungle: the Liaiblity of Internet Intermediaries for Privacy Violations in Europe", *JIPITEC* 2015, p. 214-216.

[103] B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", 2009 *Identity in the information society*, p. 62.

[104] Cf. *supra*; section B.I.4.

2. Proportional liability

52 Despite the increased number of obligations incumbent upon processors, the relationship between controllers and processors has remained largely the same. Like before, the processor is essentially conceived of as an “agent” or “delegate” of the controller, who may only process personal data in accordance with the instructions of the controller (articles 29 and 28[10]). As a result, the liability exposure of processors remains more limited in scope than the liability exposure of controllers. Whereas controllers can in principle be held liable for damages arising from *any* infringement of the GDPR, processors can in principle only be held liable in case of failure to comply with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller (article 82[2]). This is essentially a “proportional” liability model, as the processor can in theory only be held liable in relation “for his segment” in the processing.[105] The processor will be liable for the entire damage however, insofar as it is - at least partially - responsible for the harm suffered (article 82[4]). To properly understand the meaning of article 82(4), it is worth elaborating upon its legislative history.

53 In the initial proposal for the GDPR, the Commission provided that processors would be jointly and severally liable, together with any controller involved in the processing, for the entire amount of the damage.[106] Mere “involvement” in the processing would be sufficient to render the processor liable, unless the processor could prove it was not responsible for the event giving rise to the damage. The Council revised the text to differentiate between the liability exposure of controllers and processors more clearly.[107] The changes introduced by the Council, which were retained in the final version of the GDPR, made clear that a processor would only be liable in case of failure to comply with those obligations of the Regulation which are specifically directed to processors, or if it acted contrary to or outside of the lawful instructions of the controller. As a result, mere “involvement” in the processing is not sufficient to give rise to liability: the liability of the processor is conditional upon a prior finding of responsibility in causing the damage. Only in cases where the processor can be deemed responsible in accordance with paragraphs 2 and 3 of article 82 GDPR can it be held liable for the entire damage. It is important to note however, that there is no threshold regarding the *degree* of responsibility of the processor in contributing to the damage. Even if the processor is only partially responsible, the processor can be held liable for the entire amount of the damage.[108]

54 From the perspective of the data subject, article 82(4) of the GDPR results in a “cumulative” liability regime.[109] The controller carries a general responsibility for the processing and can be held liable for damages in the event of an unlawful processing activity. The data subject additionally has the possibility to sue the processor directly in case he or she has reasons to believe that the processor and not (only) the controller is in fact responsible for the damage.[110] In such cases, the data subject will effectively have a choice whether to sue the controller, the processor, or both.[111] In cases where a controller and processor have been bound to the same judicial proceedings, compensation may be apportioned according to the responsibility of

[105] See 2012/0011 (COD), 7586/1/15 REV 1, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 10 April 2015, in particular at p. 11 (Germany); p. 23-24 (France); p. 27 (Croatia) and p. 63 (Portugal). The concept of “proportional liability” is not always neatly defined and can be used to mean different things. See I. Gilead, M.D. Green and B.A. Koch, “General Report – Causal uncertainty and Proportional Liability: Analytical and Comparative Report”, in I. Gilead, M.D. Green and B.A. Koch (eds.), *Proportional Liability: Analytical and Comparative Perspectives, Tort and Insurance Law* 2013, Vol 33, p. 1 et seq. Here the term is used to signal that each party’s liability exposure is limited to their proportional share in causing the damages. If one party proves insolvent, the loss shall in principle be borne by the data subject. By contrast, in case of joint and several liability, each party can be held liable by data subjects for the full amount. See also J. Boyd and D.E. Ingberman, “The ‘Polluter pays principle’”: Should Liability be Extended When the Polluter Cannot Pay?”, *The Geneva Papers on Risk and Insurance* 1996, Vol. 21, No. 79, p. 184.

[106] COM(2012) 11, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”, 2012/0011 (COD), p. 91.

[107] 2012/0011 (COD), 9565/15, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach”, 11 June 2015, p. 185.

[108] See also 2012/0011 (COD), 9083/15, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 27 May 2015, p. 3 (“[E]ach non-compliant controller and/or processor involved in the processing are held liable for the entire amount of the damage. However a controller or processor is exempted from this liability if it demonstrates that it is not responsible for the damage (0% responsibility). Thus only controllers or processors that are at least partially responsible for non-compliance (however minor, e.g. 5%) with the Regulation, and/or in case of a processor, with the lawful instructions from the controller, can be held liable for the full amount of the damage.”).

[109] 2012/0011 (COD), 9083/15, “Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII”, 27 May 2015, p. 3.

[110] *Ibid*, p. 2.

[111] *Id.*

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.[112] In cases where the processor is not joined to the same proceeding, the controller is entitled to claim back any compensation from the processor that was paid for in damages for which the processor was responsible (article 82[5] GDPR).

55 The cumulative liability regime of article 82(4) of the GDPR reflects the Principles of European Tort Law (PETL) regarding multiple tortfeasors. According to article 9:101 of the PETL, liability is solidary "where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons".[113] The same provision also stipulates that where persons are subject to solidary liability, the victim may claim full compensation from any one or more of them, provided that the victim may not recover more than the full amount of the damage suffered by him.[114] The main innovation of the GDPR in comparison to Directive 95/46 therefore does not relate to the imposition of cumulative or solidary liability as such (as the GDPR merely codifies general tort law principles), but rather to the fact that the GDPR also imposes an increasing number of obligations directly upon processors.

56 Finally, it is worth noting that article 28(10) explicitly states that if a processor infringes the GDPR by determining the purposes and means of processing, it shall be considered to be a controller in respect of that processing. The rule of article 28(10) applies "without prejudice to articles 82, 83 and 84", meaning that a failure to abide by the controller's instructions could still give rise to liability, even if the processing might theoretically have been legitimate if the processor had obtained the data through other means. It also implies that the initial controller remains liable towards the data subject even in cases where the processor re-purposes the data.[115]

3. Burden of proof

57 To hold a processor liable, the data subject must succeed in demonstrating three elements: namely, (1) the performance of an "unlawful act" (i.e. failure to comply with those obligations of the GDPR which are specifically directly to processors or an act contrary to or outside of the lawful instructions of the controller); (2) the existence of damages; and (3) a causal relationship between the unlawful act and the damages incurred.

58 As indicated earlier, the data subject may be able to invoke one or more presumptions in order to help substantiate its claims.[116] While the GDPR does not impose upon processors a general obligation to "be able to demonstrate" compliance, processors will often still be "best placed" to provide evidence of their efforts to comply with the obligations applicable to processors. As a result, the evidential burden of proof may also shift to the processor as soon as the data subject offers *prima facie* evidence of a failure to comply with those obligations of the GDPR, which are incumbent upon processors.[117] Again, it should be noted that the ability for the data subject to avail him- or herself of such a presumption may vary according to the domestic legal system of each Member State.

4. Defences

59 Processors can in principle benefit from the same liability exemptions as controllers. A processor who is considered (at least partly) responsible for the damage may be exempted from liability - in whole or in part - if it proves that it is not in any way responsible for the event giving rise to the damage (article 82[3]).[118] In addition, processors acting as internet intermediaries within the meaning of article 12 to 15 of the E-Commerce Directive, may also be exempted from liability provided the conditions listed in these articles are met.

5. Sub-processing

60 An interesting issue to consider is the liability of processors in the case of sub-processing. Article 28(4) of the GDPR provides that in the case of subprocessing, the initial processor remains fully liable towards the controller for the performance of the relevant obligations by the subprocessor. The GDPR does not however explicitly state that the initial processor also remains liable towards the data subject. Nevertheless, the argument can easily be made that this should be the case. After all, the GDPR imposes obligations directly upon processors. Every processor involved in the processing must therefore accept personal responsibility for those requirements directed towards processors, even in the case of outsourcing. The formulation of the escape clause of article 82(3) makes clear that the GDPR also imposes a non-delegable duty of care upon

[112] Recital (146) GDPR.

[113] Art. 9:101(1) PETL.

[114] Art. 9:101(2) PETL.

[115] See also *supra*; section B.II.2.

[116] Compare *supra*; section B.I.2.

[117] Compare *supra*; section C.I.2.

[118] See also *supra*; section C.I.4.

processors.

6. Eligible damages

61 Under the GDPR, data subjects can claim both material and non-material damages from processors (article 82[1]).

III. Multiple controllers

1. Separate controllers

62 Pursuant to article 82(2) GDPR, any controller involved in the processing can in principle be held liable for the damages suffered. Read in isolation, one might assume that both joint and separate controllers face equal liability exposure. This is not the case however. While joint controllers can theoretically always be held liable for damages caused by processing activities under their joint control, separate controllers can only be held liable if the damage was caused by a processing activity which was under the control of that particular controller (or may otherwise be attributed to him). After all, article 82(4) provides that every controller involved in the processing may only be held liable "for the entire damage" insofar that they can be held responsible in accordance with paragraphs 2 and 3. As a result, separate controllers shall in principle only be liable for the entire damage if they acted as a controller towards the processing activity which gave rise to the damage or in case of "concurring faults".[119]

2. Joint controllers

63 The GDPR introduced a new provision dedicated specifically to situations of joint control. Article 26(1) provides that joint controllers must determine their respective responsibilities for compliance with the GDPR, in particular as regards to the exercise of data subject rights and their respective duties to provide information by means of an "arrangement" between them.[120] The arrangement must duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects (article 26[2]).

64 For the most part, article 26 of the GDPR can be seen as a codification of the earlier guidance provided by the Article 29 Working Party regarding the legal implications of joint control.[121] A notable difference however, is that every joint controller in principle remains liable towards data subjects for the entire damage even if there exists an appropriate arrangement between them (article 82[4]).[122] A joint controller can only escape liability if it succeeds in demonstrating that is not in any way responsible for the event giving rise to the damage (article 82[3]), or that it satisfies the conditions for liability exemption for intermediary service providers contained in Directive 2000/31 (article 2[4]).

D. Assessment

65 The GDPR has not fundamentally altered the basis for apportioning liability among organisations involved in the processing of personal data. The distinction between "controllers" and "processors" is still a decisive factor. Nevertheless, a number of important changes and clarifications have been made. From a liability perspective, the main novelties of the GDPR are:

1. the increased number of obligations directly applicable to processors and the recognition of their liability towards data subjects;
2. the formal recognition of a cumulative liability regime where more than one controller or processor are involved in the processing;
3. the incorporation of the liability exemptions contained in articles 12-15 of Directive 2000/31.

66 The liability model for controllers has essentially remained the same as under Directive 95/46: a

[119] Compare supra; section B.III.2.

[120] Joint controllers are not obliged to put in place such an arrangement in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

[121] Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 22. See also *supra*; section B.III.2.

[122] In its First Reading, the European Parliament had proposed to limit the joint and several liability between controllers and processors in cases where there existed an appropriate written agreement determining their respective responsibilities (P7_TA(2014)0212, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), p. 291. This approach was undesirable however, as it implied that the data subjects would carry the burden of determining which of the joint controllers was ultimately responsible for the damage. The revisions introduced by the Council brought the final text of the GDPR in line with the general principles of European tort law, according to which liability is solidary "*where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons*". See art. 9:101 of the Principles of European Tort Law (PETL).

controller shall in principle be liable for any damages arising from the unlawful processing personal data. The liability of the controller is also still "strict" in the sense that, once an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault. Contrary to Directive 95/46, the GDPR also explicitly recognises processor liability. The liability exposure of processors however, remains much more limited in scope than the liability exposure of controllers. Whereas controllers can in principle be held liable for damages arising from any infringement of the GDPR, processors can theoretically only be held liable in case of failure to comply with obligations of the GDPR specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the controller.

67 The cumulative liability regime of article 82(4) of the GDPR reflects the general principles of tort law regarding multiple tortfeasors. The main innovation of the GDPR in comparison to Directive 95/46 therefore does not relate to the imposition of cumulative or solidary liability as such, but rather to the fact that the GDPR also imposes an increasing number of obligations directly upon processors. The incorporation of the liability exemptions contained in Directive 2000/31 is likely to provide greater legal certainty to the providers of certain processing services, but there will still be many grey areas. In those cases, a balanced approach is necessary, which takes into account the "responsibilities, powers and capabilities" of the actor(s) in question.

68 Finally, the GDPR also explicitly recognises the eligibility of non-material damages. While this was arguably already the case under Directive 95/46, the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU Member States.

E. Conclusion

69 The liability model of EU data protection law is consistent with the Principles of European Tort Law (PETL), provided one takes into account the "general" liability of controllers and the "proportional" liability of processors. In many ways, the changes introduced by the GDPR merely constitute a (further) codification of general tort law principles.

70 The GDPR has retained the general principle that the controller carries "general" (or "primary") liability exposure for any processing activity under its control. It also recognises, in contrast to Directive 95/46, that processors should be directly liable towards data subjects. In addition, by rendering more obligations directly applicable to processors, the enforceability of certain obligations is no longer contingent upon the existence of a "contract or other legal act" between the controller and processor. The result is a cumulative liability regime, in which the data subject has a choice whether to sue the controller, the processor, or both – at least in cases where both controller and processor are at least partially responsible for the damage. In cases where the processor is not in any way responsible for the damage however, the only avenue for remedy shall be against the controller(s) involved in the processing.

71 While the GDPR has provided for greater clarity regarding the liability exposure of actors involved in the processing of personal data, it has not given special consideration to the difficult position that data subjects may find themselves in when trying to substantiate their claims. While certain data subjects may be able to avail themselves of one or more presumptions, the ability to effectively do so will depend on their domestic legal system. Absent the possibility to invoke such presumptions, the burden of proof incumbent upon data subjects remains quite onerous. The question may be asked therefore, whether it would not be desirable to formally recognise a shift in the burden of proof towards controllers and processors as soon as the data subject has offered *prima facie* evidence of an unlawful processing operation. Doing so would likely enhance the accountability of both actors towards data subjects.

* *Brendan Van Alsenoy, PhD.* is a senior affiliated researcher at the KU Leuven Centre for IT & IP Law - imec.

Acknowledgements
I would like to thank Wannes Vandenbussche, Jef Ausloos, Paul De Hert and Joelle Jouret for their valuable input and comments during the writing process. Any errors contained in the article remain my own. The research leading to this paper has received funding from the European Community's Seventh Framework Programme for research, technological development and demonstration in the context of the REVEAL project (revealproject.eu) (grant agreement no: 610928) and from the Flemish research institute imec (previously "iMinds").