

## **Liability for Damage as a Remedy for Infringement of Data Protection rights – Implications for legislation and practice in North Macedonia**

*Neda Zdraveva\**

### **Abstract**

*The Charter of Fundamental Rights of the European Union<sup>1</sup> Article 8(1) and the Treaty on the Functioning of the European Union<sup>2</sup> Article 16(1) provide that everyone has the right to the protection of personal data concerning them. The General Data Protection Regulation<sup>3</sup> operationalizes this fundamental right, laying down rules relating to the protection of natural persons when it comes to the processing of personal data and rules relating to the free movement of personal data. The GDPR provides a general right for an effective judicial remedy and a specific right to compensation for damage suffered as a result of an infringement of the Regulation. GDPR changes or adds to the landscape of the national tort law systems.*

*This paper provides an overview and analysis of the key features of the non-contractual liability for a data breach as provided by the GDPR. It also identifies several issues that may lead to differences in the application of the GDPR in the Member States. The key issues at stake are first whether and how the liability for damage, as a remedy provided in GDPR, influences the legislation in North Macedonia, a candidate country, and second how it may influence the implementation of this remedy in the practice. The author concludes that the mechanisms existing in the national legislation provide for an effective and efficient remedy of the data protection rights.*

---

\* Prof. Assoc. Dr. Neda Zdraveva is a full time professor at the Institute for Civil Law at Iustinianus Primus Law Faculty, Ss. Cyril and Methodius University in Skopje. Her main areas of research are in Contract Law, Consumer Law and Intellectual Property Law.

<sup>1</sup> Charter of Fundamental Rights of the European Union, OJ C 326 (hereafter: Charter)

<sup>2</sup> Treaty on the Functioning of the European Union, OJ C 326 (hereafter: TFEU)

## 1. Introduction

The Charter of Fundamental Rights of the European Union<sup>4</sup> Article 8(1) and the Treaty on the Functioning of the European Union<sup>5</sup> Article 16(1) provide that everyone has the right to the protection of personal data concerning them. TFEU stipulates that the European Parliament and the Council, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data (Article 16(2)) while the Charter states that the processing must be “fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” (Article 8(2)). The General Data Protection Regulation<sup>6</sup> operationalizes these fundamental rights, laying down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.<sup>7</sup> GDPR provides a general right for an effective judicial remedy (Article 79) and for a specific right of compensation for damage caused by an infringement of the Regulation (Article 82). This right to compensation is set out as a civil liability mechanism. In this regard, data protection is considered a rather privileged field, as the GDPR not only enshrines a general right to an effective judicial remedy, but also a specific right to compensation for damage caused by a breach of the Regulation’s provisions.<sup>8</sup> The right to compensation for is not a novelty in the data protection legislation of the EU. The Data Protection Directive<sup>9</sup> provided for a similar right to compensation under Article 23(1), requiring Member States to provide that “any person who has suffered

---

<sup>4</sup> Charter of Fundamental Rights of the European Union, *OJ C 326* (hereinafter: Charter)

<sup>5</sup> Treaty on the Functioning of the European Union, *OJ C 326* (hereinafter: TFEU)

<sup>6</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119* (hereinafter: GDPR)

<sup>7</sup> Article 1(1), GDPR

<sup>8</sup> Zanfir- Fortuna G., “Article 82. Right to compensation and liability” in: Kuner C., Bygrave L.A., Docksey C. (eds.); *The EU General Data Protection Regulation (GDPR) - A Commentary*, Oxford University Press, Brussels and Oslo, 2019, p. 1163

<sup>9</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281* (hereinafter DPD)

damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the controller for the damage suffered". The GDPR however, goes further in detailing the scope and the approaches to civil liability for damage suffered as a result of unlawful processing of the personal data. The Law Enforcement Directive<sup>10</sup> Article 56 includes a right to compensation, which stipulates an obligation for the Member States to provide "for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law".

Placed among the administrative law mechanisms protecting one's personal data, Article 82 of the GDPR provides very specific rules for the establishment of liability and liable party/ies, making the issue fall within the ambit of the Civil Law (Law on Obligations, Tort Law) *per se*. Thus, the GDPR changes the landscape of the national tort law systems, as the regulations are binding in its entirety and directly applicable in all Member States<sup>11</sup> and their provisions usually have direct effect, including between private parties, as long as they are sufficiently clear, precise and relevant to the situation of an individual litigant.<sup>12</sup> However, it could be argued that the national legislation of the Member States would need an express provision for a claim of compensation *inter alia*, due to lack of clarity of the provision. Article 82(1) that uses the phrase "Any person who has suffered material or non-material damage .... shall have the right to receive compensation ... "instead of the term "has a right". This, as argued, "provokes both the question 'how shall the plaintiff have compensation?' and the answer

---

<sup>10</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119* (hereinafter LED)

<sup>11</sup> Art. 288 Treaty on the Functioning of the European Union (TFEU).

<sup>12</sup> Craig P., de Búrca G.; *EU Law: Text, Cases, and Materials*; Oxford University Press, 2015, p. 198 and the relevant case law

that further steps must be taken before a plaintiff actually has the claim.”<sup>13</sup> As a result, national incorporating legislation “is clearly necessary to clarify that such a claim is available, and to ensure that it is coherent and comprehensible to those who would seek to rely on it.”<sup>14</sup>

However, even if national legislation implementing or further specifying Article 82 does not exist, or Article 82 is implemented in a way that is not compatible with the GDPR, the national courts or the authorities that decide upon claims for damage can apply Article 82 directly. The data breach would, therefore, constitute a non-contractual relationship between the person who suffers the damage and the liable person, and this relation would be primarily governed by the rules of the GDPR. The liability for damage foreseen by the GDPR “discourage[s] practices, frequently covert, which are liable to infringe the rights of data subjects, thereby making a significant contribution to the protection of privacy and data protection rights in the European Union”.<sup>15</sup>

The Constitution of the Republic of North Macedonia Article 18 guarantees the security and confidentiality of personal information. The citizens have protection from any violation of their personal integrity deriving from the registration of personal information through data processing.<sup>16</sup> The Stabilisation and Association Agreement signed between the European Communities and their Member States, of the one part, and the Republic of North Macedonia, of the other part<sup>17</sup> recognizes the ‘importance of the approximation of

---

<sup>13</sup> O'Dell E., Compensation for Breach of the General Data Protection Regulation, Dublin University Law Journal, vol. 40, no. 1, 2017, p. 111

<sup>14</sup> O'Dell E., *ibid*, p. 122

<sup>15</sup> O'Dell, E., *ibid*, p. 101

<sup>16</sup> Constitution of the Republic of North Macedonia and Amendments I - XXXVI (“Official Gazette of the Republic of Macedonia” no. 1/92, 31/98, 91/01, 84/03, 107/05, 3/09, 49/11, 6/19, 36/19)

<sup>17</sup> Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the former Yugoslav Republic of Macedonia, of the other part - Protocol 1 on textile and clothing products - Protocol 2 on steel products - Protocol 3 on trade between the former Yugoslav Republic of Macedonia and the Community in processed agricultural products - Protocol 4 concerning the definition of the concept of “originating products” and methods of administrative

the existing and future laws of North Macedonia to those of the Community.<sup>18</sup> This, in the field of data protection, was reflected in the first Law on Data Protection that provided for the implementation of the Data Protection Directive in the legislation of North Macedonia.<sup>19</sup> In 2020 a new law was enacted, harmonizing the national data protection legislation with the GDPR. The Law regulates the protection of personal data and the right to privacy with regard to the processing of personal data, and in particular the principles related to the processing of personal data, the rights of the data subject, the position of the controller and the processor, the transfer of personal data to other countries, the establishment, status and competencies of the Personal Data Protection Agency, the special operations for the processing of personal data, the legal remedies and liability in the processing of personal data, the supervision over personal data protection, as well as the misdemeanours and misdemeanour proceedings in this area.<sup>20</sup> With regard to the legal remedies and liability, the LDP Article 101 provides for liability for damage in case of a breach of the provisions protecting personal data. The law stipulates that a number of its provisions, including those regulating the liability for data infringement, will cease to apply with the accession of North Macedonia to the European Union<sup>21</sup>, resulting in the GDPR being

---

cooperation - Protocol 5 on mutual administrative assistance in customs matters - Final Act, *OJ L 84, 20.3.2004, p. 13–197* (hereinafter SAA). When the SAA was signed the reference 'former Yugoslav Republic of Macedonia' was used as per United Nations General Assembly Resolution 47/225 of 27 April 1993. Following the Final Agreement for the settlement of the differences as described in the United Nations Security Council Resolutions 817 (1993) and 845 (1993), the termination of the Interim Accord of 1995, and the establishment of a Strategic Partnership between the Parties, the official name of the state is Republic of North Macedonia

<sup>18</sup> Article 68(1), SAA

<sup>19</sup> Law on Data Protection („Official Gazette of Republic of Macedonia no. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18); hereinafter: LDP

<sup>20</sup> Article 1, LDP

<sup>21</sup> It is very important here to note that the provision of the Law regulating the termination of application (Article 122) reads: "The provisions of Chapter II (except Article 12), III, IV (except Articles 46 and 47), V and VIII of this Law shall cease to apply until the accession of the Republic of North Macedonia to the European Union." The provision in relation to the general aim of the law to provide for approximation with the GDPR is to be understood that the application of the enlisted parts of the law will cease with the accession to the EU. In order to provide for clarity of the provision, the

directly applicable in national law. The right to compensation is to be exercised in court proceedings in accordance with law. The applicable law regulating the obligations arising from damage is the Law on Obligations<sup>22</sup> as a general law. In the Macedonian legal theory, the obligations arising from damage (civil wrongs, torts) are defined as a relation in which for the tortfeasor an obligation to compensate the damage arises, while the injured party has a right to compensation for the damage endured. <sup>23</sup> For the obligation to arise under the law of North Macedonia there need to be two parties (injured and tortfeasor), there general conditions (elements), damage, wrongful/unlawful act and casual link between them, must be met, and the specific condition of an existence of fault on the side of the tortfeasor or dangerous object or activity must be fulfilled. In this, the Tort Law of North Macedonia follow the general concepts of continental tort law. Having this in mind the paper further will examine the conditions of tort under law of North Macedonia from the perspective of the GDPR and the position of the national legislation vis-à-vis the GDPR. In the national legal theory, the issue of civil liability for a data breach has not been analysed yet.

## 2. Parties to the Obligation

### 2.1. Injured Party

Stating that “[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right ...”, Article 82(1) GDPR defines the injured party. However, the definition is not as simple as it may seem. Who is protected and thus, potentially an injured party and claimant? There

---

Ministry of Justice on 16.03.2021 proposed enactment of Law on Amendments of the LDP that foresees the word “until” in Article 122 to be replaced with the word “with” meaning the stated Article would read: “The provisions of Chapter II (except Article 12), III, IV (except Articles 46 and 47), V and VIII of this Law shall cease to apply with the accession of the Republic of North Macedonia to the European Union.”

<sup>22</sup> Law on Obligations (“Official Gazette of the Republic of Macedonia” no. 8/2001; 4/2002; 5/2003; 84/2008; 81/2009 and 161/2009); hereinafter: LOO

<sup>23</sup> Галев Г., Дабовиќ – Анастасовска Ј., Облигационо право, Правен факултет „Јустинијан Први“ – Скопје, Скопје, 2009, стр. 583 (Galev, G., Dabovikj – Anastasovska J. Law of Obligations, Iustinianus Primus Law Faculty – Skopje, Skopje, 2009, p. 583)

are three answers possible: 1) natural and legal persons, 2) only natural persons or 3) the specific data subject as a natural person.

When it comes to the protection in relation to the processing of personal data, the GDPR awards it to natural persons,<sup>24</sup> regardless of their nationality or place of residence.<sup>25</sup> It is clear that the GDPR does not protect legal persons, as it does not “cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person”.<sup>26,27</sup> The specific protection is afforded to an identified or identifiable natural person whose personal data (any information related to them) was processed, the data subject.<sup>28</sup> An “identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”, and information related to this constitutes the term ‘personal data’.<sup>29</sup> In determining whether a natural person is identifiable, the GDPR states that one should take into account all the means reasonably likely to be used to identify the natural person directly or indirectly, having in mind ‘all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments’<sup>30</sup>. The term ‘natural person’ is still wider than the term ‘data subject’ also used in the GDPR, as it may include third persons who are not the data subject,

---

<sup>24</sup> Article 1(1), Recital 1, GDPR

<sup>25</sup> Recital 14, GDPR

<sup>26</sup> Recital 14, GDPR

<sup>27</sup> Vicente D.M., Vasconcelos Casimiro S.; “Data Protection in the Internet: General Report”, in: Vicente D.M., Vasconcelos Casimiro S., (eds.); *Data Protection in the Internet, Ius Comparatum – Global Studies in Comparative Law*, Volume 38, Springer, 2020, p.8

<sup>28</sup> Article 4(1/4), Recital 25, 1<sup>st</sup> sentence, GDPR

<sup>29</sup> Article 4(1/4), Recital 25, 1<sup>st</sup> sentence, GDPR

<sup>30</sup> Recital 26, GDPR

but would potentially have a legal interest when specific data of the data subject is not processed in accordance with the GDPR.

The position of the legislator in GDPR is not a clear one. For example, in recital 146 it uses both terms 'person' and 'data subject', providing, on one hand, obligation damage to be compensated to 'a person that suffer as a result of processing that infringes the regulation'<sup>31</sup>, and on the other that 'full and effective compensation for the damage suffered to be provided to the data subjects'<sup>32</sup>.

The views on who may be the injured party and claimant differ. One position is that only the data subject may receive compensation. This is based on the arguments that a) the purpose of the GDPR is the protection of data subjects, b) recital 146 sentence 6 places the right to compensation with the data subject, c) Article 82(2) presuppose a causal link between the (wrongful) processing of personal data and the damage, d) the controllers and processors have primary obligations to protect the data subjects and their data. Another view is that the notion "all persons" should be interpreted in a broader manner, to also include persons who have a legal interest in the processing data of the data subject. The argument is based on a) the reference to data protection right as a fundamental right that all natural persons enjoy, b) that GDPR Article 82 operates with the term 'any person' while in other articles uses more specific terms such as 'any natural person' or 'data subject', and c) that the duties that controllers and processors have are duties not only towards the data subjects but also more general ones, etc.<sup>33</sup>

The terms 'any person' or 'a person' are relatively common expressions when it comes to defining who has the right to damages<sup>34</sup> in civil law, and interpretations and conclusions should not be drawn from the term alone. The protection of natural persons is undisputed. It is also a fact that a third party might have a valid legal interest in the

---

<sup>31</sup> Recital 146, 1<sup>st</sup> sentence, GDPR

<sup>32</sup> Recital 146, 6<sup>th</sup> sentence, GDPR

<sup>33</sup> On different position see further Mendezes Cordeiro A. B., *Civil Liability for Processing of Personal Data in the GDPR*, *European Data Protection Law Review (EDPL)*, vol. 5, no. 4; 2019, p. 493.; Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017, p. 206

<sup>34</sup> See VI.- I:101 (1) of Draft Common Frame of Reference.



processing of data of another person and that they might suffer damages when such processing is unlawful. From a perspective of substantive civil law, the provision of Article 82(1) GDPR would be read as applying to any person not just the data subject so that this mechanism is available to any person that can prove a causal link between the wrongful act and the damage. However, Article 79(1) GDPR is of a procedural nature and provides for the right to an effective judicial remedy to the data subject, meaning that active right to a claim for compensation in a judicial procedure will be with the data subject. Furthermore, Article 80(1) GDPR, dealing with the issue of representation, provides the data subject with the right to mandate a non-profit body, organisation or association to *inter alia* exercise the right to receive compensation on their behalf. Having said this, we find that the narrow interpretation of Article 82 (1) GDPR is more likely to be applicable by the national courts and authorities.

## **2.2. Liable Party**

Article 82(2) GDPR identifies the controller and the processor as liable party(ies), stipulating “Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.” Processing personal data in terms of Article 4(1/2) GDPR means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

As per Article 4(1/7) GDPR ‘controller’ means “(i) the natural or legal person, public authority, agency or other body which, (ii) alone or jointly with others, (iii) determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”. The first element of the definition

of controller should be interpreted broadly to include any person regardless of their status or form of establishment, but it is important that this person “determines purposes and means of the processing of personal data”, as provided in Article 4(1/7) GDPR. In this context the focus is on the person that does the actual processing, and when this is a legal person, that legal person will be held liable. Any employees or persons acting on behalf of the legal person may be liable under the national rules for liability of employees. Article 4 (1/8) GDPR defines the ‘processor’ as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The fact that the processor can be directly held liable for violations of its obligations under the GDPR is an important novelty. When a controller and a processor are involved in data processing, Article 82(2) GDPR provides for a system of liability that takes account of the different roles of controllers and processors in data processing activities. Thus, the controller bears the liability for unlawful processing and has to compensate the damage irrespective of whether the controller directly caused the damage or it is a result of the instructions, for example, provided to the processor. This arises from the controller’s role to determinate the purposes and means of the processing, regardless of whether they act on their own or through a third party processor. The processor acting on behalf of the controller will be liable only when the damage is a result of breaches of the processors obligations under the GDPR or where it acted contrary to the obligations of the controller that arise from the “contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller”.<sup>35</sup>

Article 82(4) GDPR establishes that controllers and processors are jointly and severally liable for the damage, to the extent they are responsible for the unlawful processing causing the damage. Although the text of the GDPR does not contain the words joint and several, it is clear that this was the lawmakers' intention, through both a literal interpretation of the text of the provision and from a teleological interpretation.<sup>36</sup> Where more than one controller or processor, or both a controller and a processor, “are involved in the same processing” and

---

<sup>35</sup> Article 28(3), GDPR

<sup>36</sup> Menezes Cordeiro A.B., *ibid*, p. 499

they are responsible for any damage caused by that processing, “each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject”<sup>37</sup>. Providing for the joint and several liability of the controller(s) and the processor(s), the GDPR puts into effect the goal of the compensatory measures to provide for “full and effective compensation of the data subject”<sup>38</sup> and further reinforces the fundamental right to effective judicial protection, provided by Article 47 of the Charter, in connection to the right to personal data protection, provided by Article 8 of the Charter. At the same time, the GDPR allows compensation to be “apportioned according to the responsibility of each controller or processor for the damage caused by the processing”.<sup>39</sup> In accordance with Article 82(5) GDPR, if one of the entities held jointly and severally liable for compensation of damages pays the full compensation for the damage suffered it has the right “to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage incurred”. The provision of the joint and several liability on the controller and the processor, “... viewed positively provides that throughout the collection, use and management of personal data, someone is accountable. However, a problem could arise where their respective responsibilities are not clearly defined and have been blurred.”<sup>40</sup>

When it comes to the issue of the jurisdiction, the incurred party has the right to choose the venue, except when the controller is a public authority of a Member State acting in the exercise of its public powers. In accordance with Article 82(6) GDPR in conjunction with Article 79(2) GDPR, regulating proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member State where the controller or

---

<sup>37</sup> Recital 146, 7<sup>th</sup> sentence, GDPR

<sup>38</sup> Recital 146, 6<sup>th</sup> sentence, GDPR

<sup>39</sup> Recital 146, 8<sup>th</sup> sentence, GDPR

<sup>40</sup> Walters R., Trakman L., Zeller, B.; *Data Protection Law: A Comparative Analysis of Asia Pacific and the European Union*, Springer, 2019. p. 60

processor has an establishment or alternatively, where the data subject has his or her habitual residence.<sup>41</sup>

### 3. Elements of the Civil Liability

#### 3.1. Wrongful/Unlawful Act

Article 82(1) GDPR provides a broad ground for establishment of what will be considered a wrongful act, stipulating that the damage should be a “result of an infringement of this Regulation”. Such position of the GDPR is not a novelty, as Article 23(1) of the DPD requires the Member States to provide for liability when there was a damage arising from “an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive”. In addition to violations of the GDPR, Article 82 covers “processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation”.<sup>42</sup> This provision does not limit the remedies available for violations of the GDPR, as it is without prejudice to any claims for damages deriving from violations of other rules in Union or Member State law, that may *inter alia* include liability for breaches of contracts depending on the scope of the act or omission that resulted in the damage.

What are the specific obligations of the controller and the processor for which an infringement may be considered an unlawful act and constitute basis for liability? The GDPR defines the principles of data procession and when processing will be considered lawful. Thus, any act or omission that violates the principles of data processing, or any breach of the conditions for its lawfulness, may be considered an unlawful act that can give rise to a claim for compensation for damages.

GDPR sets out several principles<sup>43</sup> for data processing, for which the controller is responsible and should be able to demonstrate compliance with The principles require the procession of personal

---

<sup>41</sup> See also Recital 145

<sup>42</sup> Recital 146, 5<sup>th</sup> sentence, GDPR.

<sup>43</sup> Article 5, GDPR

data to be: 1) lawful and fair<sup>44</sup>; 2) transparent as to how personal data concerning natural persons are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed, including the identity of the controller and the purposes of the collection.<sup>45</sup> This information is to be provided in an easily accessible and understandable manner, with clear and plain language used<sup>46</sup> and the natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data, as well as how to exercise their rights in relation to such processing;<sup>47</sup> 3) adequate, relevant and limited to what is necessary for the purposes for which they are processed,<sup>48</sup> including limited in time,<sup>49</sup> where the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data;<sup>50</sup> 4) processed only if the purpose of the processing could not be reasonably fulfilled by other means;<sup>51</sup> 5) kept only as long as necessary, this purpose time limits should be established by the controller for erasure or for a periodic review;<sup>52</sup> 6) rectified or deleted if they are inaccurate;<sup>53</sup> 7) processed in a manner that ensures appropriate security and confidentiality of the personal data, including preventing unauthorised access to or use of personal data and the equipment used for the processing.<sup>54</sup>

As per Article 6, processing is lawful only if and to the extent that at least one of the following applies: 1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. The GDPR provides specific rules for determining when a

---

<sup>44</sup> Article 5 (1/a), Recital 39, 1st sentence, GDPR

<sup>45</sup> Recital 39, 4<sup>th</sup> sentence, GDPR

<sup>46</sup> Article 5 (1/a), Recital 39, 2<sup>nd</sup> and 3<sup>rd</sup> sentence, GDPR

<sup>47</sup> Recital 39, 5<sup>th</sup> sentence, GDPR

<sup>48</sup> Recital 39, 7<sup>th</sup> sentence, GDPR

<sup>49</sup> Recital 39, 8<sup>th</sup> sentence, GDPR

<sup>50</sup> Recital 39, 6<sup>th</sup> sentence, GDPR

<sup>51</sup> Recital 39, 9<sup>th</sup> sentence, GDPR

<sup>52</sup> Recital 39, 10<sup>th</sup> sentence, GDPR

<sup>53</sup> Recital 39, 11<sup>th</sup> sentence, GDPR

<sup>54</sup> Recital 39, 12<sup>th</sup> sentence, GDPR

consent will be considered valid.<sup>55</sup> In brief it requires the data subject to be informed in an intelligible and easily accessible form, using clear and plain language, about the processing of the data and the right to withdraw the consent. The data subject is free to choose if they will provide such consent and/or later withdraw it; 2) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation to which the controller is subject; 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; 5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and 6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, except when processing carried out by public authorities in the performance of their tasks.

When it comes to processing that is deemed necessary for compliance with a legal obligation to which the controller is subject and processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller<sup>56</sup>, Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing, including for other specific processing situations<sup>57</sup>. The basis for this processing, as

---

<sup>55</sup> Article 7, GDPR

<sup>56</sup> Article 6(2), GDPR

<sup>57</sup> This includes the related to ensuring freedom of expression and information (Article 85), public access to official documents (article 86), processing of the national identification number (Article 87), processing in the context of employment (Article 88), processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89), situations where controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy (Article 90) and data protection rules of churches and religious associations (Article 91)

per Article 6(3) GDPR is to be laid down by EU law or the law of the Member State to which the controller is subject. The GDPR provides for clear rules regarding the purpose of the processing and specific provisions to adapt the application of GDPR rules that this EU law or the Member States law should contain<sup>58</sup>.

Where the processing for has a purpose other than that for which the personal data have been collected and that processing is not based on the consent given by data subject or was authorised by Union or Member State law<sup>59</sup>, the controller has to ascertain whether the processing is compatible with the purpose for which the personal data was initially collected. Doing so the processor has to take into account, inter alia: 1) any link between the purposes for which the personal data was initially collected and the purposes of the intended further processing; 2) the context in which the personal data was collected, in particular regarding the relationship between the data subjects and the controller; 3) the nature of the personal data, in particular whether special categories of personal data were/will be processed<sup>60</sup>, or whether personal data related to criminal convictions and offences is processed;<sup>61</sup> 4) the possible consequences of the intended further processing for the data subjects; and 5) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

### **3.2. Damage**

‘Damage’ under Art. 82(1) of the GDPR includes both material and non-material damage that is a result of the unlawful act. Other than

---

<sup>58</sup> See Article 6(3), 2<sup>nd</sup> sentence, GDPR

<sup>59</sup> The law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives set in Article 23 of GDPR that define the restrictions on the scope of the right of the data subject (Article 12 -24, GDPR) and the obligation of the controller in regard to Communication of a personal data breach to the data subject

<sup>60</sup> Pursuant to Article 9, GDPR, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. The application is excluded in a limited number of situations defined by Article 9(2).

<sup>61</sup> See Article 10, GDPR

stating that it provides that “data subjects should receive full and effective compensation for the damage they have suffered”<sup>62</sup> and that “the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation”,<sup>63</sup> the GDPR does not define the damage. Still, the GDPR is more developed than previous legislation when it comes to what constitutes damages that may arise due to data breach. The DPD Article 23(1) referred only to ‘damage’ without specifying whether that meant material and/or non-material damage. As a result, the national law transposing DPD in the Member states varied. In Greece for example, it included both material and non-material damage, in Germany only material damage or pecuniary loss was covered, while in the UK compensation for distress (understood as non-material damage) could be awarded if the individual ‘also suffers damage’ (understood as material damage).<sup>64</sup> The specification of the damage and in particular the introduction of non-material damage arose in the legislative process. The European Data Protection Supervisor, in their Opinion on the data protection reform, was of the opinion that “it would also be appropriate to provide for the compensation of immaterial damage or distress, as this may be particularly relevant in this field.” However, the introduction of the concept of damage understood as both material and non-material concept was not without concerns by the members states. Ireland, Poland and Greece had reservations on the whole article regulating the right to compensation and liability. Germany, Netherlands and the UK have queried whether there was an EU concept of damage and compensation or whether this was left to Member State law. Italy suggested specifying that the rules on liability are to be applied according to national law, which was supported by the Czech Republic, the Netherlands, Romania and Slovenia. The position of the

---

<sup>62</sup> Recital 146, 6<sup>th</sup> sentence, GDPR

<sup>63</sup> Recital 146, 2<sup>nd</sup> sentence, GDPR

<sup>64</sup> See further Truli, E., “The General Data Protection Regulation and Civil Liability” in: Mohr Backum et al., *Personal Data in Competition, Consumer Protection and Intellectual Property: Towards a Holistic Approach?* Springer, 2018, p. 313-314



Commission was that it should be left to ECJ to interpret these rules and concepts.<sup>65</sup>

In the end the GDPR was adopted with provision for compensation of both material and non-material loss, without specific definitions of the concept(s). It does provide, however, for a number of examples of what such damage may be, such as loss of control over personal data or limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.<sup>66</sup> Furthermore, the processing rights to data protection remain intrinsically linked to the right to privacy, and although the GDPR does not have any reference to the right of privacy, privacy will continue to form an integral part of the right to data protection. Moreover, "as privacy is a general principle of EU law, the Court could continue to apply the provisions of data protection regulation in light of this general principle, irrespective of whether the Regulation refers to it directly."<sup>67</sup>

### **3.3. Causal Link**

The controller and/or the processor of personal data may be liable for the damage caused by an infringement of data protection, provided there is a causal link between the wrongful act (or omission) and the damage suffered by the data subject. Article 82(1) GDPR requires the damage to be 'a result of an infringement'. The causal link represents the relation between the wrongful act and the damage - it is the connection between the event for which one of the parties is liable and the harmful consequences of that event suffered by the other. The wrongful act should be of a nature that is appropriate for the specific consequence of the case to occur, without influence of other factors.

---

<sup>65</sup> Council of the European Union, 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, doc 9788/15, note 593, p. 244

<sup>66</sup> Recitals 75 and 85, GDPR

<sup>67</sup> Lynskey O., *The Foundations of EU Data Protection Law*, Oxford University Press, 2015, p.266

Determining the adequate causal link is the task of the court, who should consider all of the circumstances and decide if the data breach is adequate to have caused the damage claimed by the injured party. One of the characteristics of the adequate causality is in the fact that the existence of wrongful act is not assumed, but proven, and the burden of proof is on the injured party. Exceptions to this rule are cases of liability for damage regardless of fault – the ‘strict’ or ‘objective’ liability. In these cases, adequacy is assumed, but the assumption is rebuttable. As presented in this paper, this would be the case for the liability for a data breach.

### **3.4. Fault Based or Strict Liability for Damage**

Article 82 GDPR does not provide reference to the ground for liability i.e., whether the liability will be based on fault, or the liability for a data breach will be a case of strict liability. Article 82(2) requires the controller to be ‘involved in processing’ and does not require intent or negligence on their side for liability to be established. In addition, the principle of accountability (Article 5(2) GDPR) requires the controller to be responsible for, and be able to demonstrate, compliance with the (other) principles relating to processing of personal data. The rule related to the exemption from liability of the controller or processor, as specified in Article 82(3) GDPR, requires them to ‘prove[s] that [they are] not in any way responsible for the event giving rise to the damage’. The controller or the processor could prove this by demonstrating occurrence of an event which caused the damage and which cannot be attributed to them. All of this leads to the conclusion that the GDPR foresees the concept of strict liability for the damage caused by a data breach. The aim of the liability exemption is “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”.<sup>68</sup> This is in line with the (theoretical) view that “many strict liability rules are explained on the basis that the defendant is in the best position to control an activity under his control and to prevent occurrence of

---

<sup>68</sup> Van Alsenoy, B.; Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 7, no. 3, December 2016, p.276

harm”.<sup>69</sup> The classification of the liability for a data breach as strict liability “is also supported by the accountability principle, which provides that the controller is responsible for demonstrating compliance with the principles relating to the processing of personal data under the GDPR, meaning that any unlawful processing is imputable to the controller, regardless of intention, fault or negligence.”<sup>70</sup> There are those however, who argue that the data entity should be liable for the reasonable consequences of its actions i.e. liability should exist when data collectors or processors reasonably foresaw harm to the data subjects.<sup>71</sup> The characterisation of the controller’s liability as strict liability is “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”.<sup>72</sup> It is also relevant in regard to the establishment of the existence of a causal link as discussed above . Keeping in mind the differences that exist in the European tort law systems, in particular when it comes to the compensation for non-material damage, it is important to establish that the courts shall not seek proving fault and shall provide compensation even for the non-material damage.

### **3.5. Assessment of the Damage**

GDPR, as expected, does not provide any rules for the national courts to apply when assessing the material and the non-material damage. The national courts in these cases should apply the national rules having in mind that “the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation.”<sup>73</sup> As the liability rules of the DPD were not subject to revision of the Court of

---

<sup>69</sup> See further Werro F., Palmer V. V., Hahn A., “Strict Liability in European tort law: an introduction” in Werro F., Palmer V. V. (eds.), *The Boundaries of Strict Liability in European Tort Law*, Carolina Academic Press, 2004, p.6

<sup>70</sup> Zanfir- Fortuna G., *ibid*, p. 1176

<sup>71</sup> Trakman L., Walters R., Zeller, B., Tort and data protection law: Are there any lessons to be learnt?, *European Data Protection Law Review (EDPL)*, vol. 5, no. 4, 2019 p. 518

<sup>72</sup> Van Alsenoy B.; *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019, p. 77

<sup>73</sup> Recitals 146, 3<sup>rd</sup> sentence, GDPR

Justice there are no specific interpretations that might provide for direct guidance for the national courts in this regard. However, in principle ECJ jurisprudence provides that compensation or reparation (caused by a breach of personal rights) should be genuine and effective in a way which is dissuasive and proportionate<sup>74</sup> and have a genuine deterrent effect on the liable party and subsequent infringers<sup>75</sup>.

#### 4. Civil Liability vs. Administrative Liability

The GDPR provides for administrative mechanisms for protection of the fundamental rights and freedoms of natural persons in relation to data protection. They range from corrective<sup>76</sup> and advisory<sup>77</sup> measures to fines and penalties. Article 83 prescribes the conditions for imposing administrative fines and their amount, specifying that they are imposed in addition to, or instead of the corrective measures.<sup>78</sup>

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, the competent national body should take into account a number of circumstances related to the acts or omissions of the controller by which the infringement was done. They include<sup>79</sup>: a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; b) the intentional or negligent character of the infringement; c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; d) the degree of responsibility of the controller or

---

<sup>74</sup> C-407/14, *María Auxiliadora Arjona Camacho v Securitas Seguridad España, SA*, ECLI:EU:C:2015:831,

<sup>75</sup> C-407/14, para. 31 and cited cases there

<sup>76</sup> See include warnings, reprimands, compliance orders, communication orders, temporary or definitive limitation including a ban on processing, certification withdrawal etc. as provided in Article 58(2), GDPR.

<sup>77</sup> Article 58(3/1), GDPR

<sup>78</sup> Article 83(2), GDPR

<sup>79</sup> Article 83(2), GDPR

processor, taking into account technical and organisational measures implemented by them; e) any relevant previous infringements by the controller or processor; f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; g) the categories of personal data affected by the infringement; h) the manner in which the infringement became known to the supervisory authority, in particular whether and to what extent, the controller or processor gave notification of the infringement; i) compliance with previously ordered corrective measures; j) adherence to approved codes of conduct or approved certification mechanisms pursuant; and k) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. The GDPR provides for administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher<sup>80</sup> in cases of breach of<sup>81</sup>: a) the obligations of the controller and/or(?) the processor<sup>82</sup>; b) the obligations of the certification body<sup>83</sup>; and c) the obligations of the monitoring body.<sup>84</sup> For the cases of breach of: a) the basic principles for processing, including conditions for consent;<sup>85</sup> b) the data subjects' rights<sup>86</sup>; c) the transfers of personal data to a recipient in a third country or an international organisation<sup>87</sup>; and d) any obligations pursuant to Member State law<sup>88</sup> as well as for non-compliance with an order of the competent authority<sup>89</sup> administrative fines up to 20 000

---

<sup>80</sup> Article 83(3), GDPR

<sup>81</sup> Article 83(4), GDPR

<sup>82</sup> Pursuant to Articles 8, 11, 25 to 39 and 42 and 43 of GDPR

<sup>83</sup> pursuant to Articles 42 and 43 of GDPR

<sup>84</sup> pursuant to Article 41(4) of GDPR

<sup>85</sup> Pursuant to Articles 5, 6, 7 and 9 of GDPR

<sup>86</sup> Pursuant to Articles 12 to 22 of GDPR

<sup>87</sup> Pursuant to Articles 44 to 49 of GDPR

<sup>88</sup> Adopted under Chapter IX of the GDPR, see note 40

<sup>89</sup> It includes non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1) (Article 83(4)(e) and

000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, is foreseen.

How will the civil court be affected by the rules related to the administrative sanctioning? Except for the grounds of liability (intent or negligence) the civil court may and probably will take into consideration the circumstances pertinent to the case in the assessment of the compensation. This will particularly be case for the nature, gravity and duration of the infringement, which is of specific relevance to the non-material damage, as well as the actions, if any, taken by the controller or processor to mitigate the damage suffered by data subjects.

According to some reports<sup>90</sup>, a total 292 million euros in fines has been imposed since the implementation of the GDPR starting in May 2018; where the highest was the fine imposed by the French National Commission on Informatics and Liberty (CNIL), amounting to 50 million euros, on the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding personalized adds. Even though the individual compensations awarded by national courts so far, according to reports, have only gone up to 5,000 euros,<sup>91</sup>the number of persons affected by a particular infringement may be large and thus, the risk of financial losses for the controllers is not insignificant.

## 5. Case: North Macedonia

The LDP has the transposed Article 82(2) GDPR *ad verbatim*. Article 101, para. 1 LDP, provides that any person who has suffered material or non-material damage as a result of an infringement of this Law is

---

non-compliance with an order by the supervisory authority as referred to in Article 58(2) (Article 83(5))

<sup>90</sup> 5 biggest GDPR fines so far, Data Privacy Manager, <https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/> [last access 25/04/2021]

<sup>91</sup> See report GDPR Violations in Germany: Civil Damages Actions on the Rise, available at <https://www.jdsupra.com/legalnews/gdpr-violations-in-germany-civil-84570/> [last access 25/04/2021]

entitled to compensation from the controller or processor for the damage suffered. As per para. 6 of Article 101 the court proceedings for exercising the right to receive compensation shall be brought before a competent court in accordance with the law. In this regard the substantive issues related to the compensation of the damage sustained because of a data breach are regulated by the Law on Obligations (LOO).

The LOO does not have a specific provision on 'data protection' *per se*, but provides for a general protection of the personal rights including the right to privacy. Thus, Article 9-a, para. 1 of LOO, provides that every natural person, in addition to the protection of property rights, has the right to protection of his personal rights in accordance with law. The LOO (Article 9-a) does not have an exhaustive list of personal rights, but provides that they are to be understood as the rights of life, physical and mental health, honour, reputation, dignity, personal name, privacy of personal and family life, freedom, intellectual creation and other personal rights.

## **5.1. Parties**

As in the GDPR the protection under the LDP is afforded to the natural persons as data subjects (an identified or identifiable natural person).<sup>92</sup> The national law in this regard does not differ from the GDPR and as discussed, the courts will, or at least should, adopt the narrow approach in interpreting who the injured party would be. Differences also do not exist in relation to the issue of the tortfeasor. LDP Article 101 identifies the controller and/or the processor<sup>93</sup> as liable for the damage. As per Article 101, para. 2, a controller who has processed the data contrary to the LDP shall be liable for the damage caused. The processor shall be liable where it has not complied with obligations of the LDP specifically directed to the processors or where it has acted outside or contrary to lawful instructions of the controller. Joint and several liability is foreseen for the cases when where more than one controller or processor, or both a controller and a processor, are

---

<sup>92</sup> Article 4, para. 1, item 1, LDP

<sup>93</sup> The definitions of controller and processors as provided in Article 4, para 1, LDP correspond to those provided in the GDPR

involved in the same processing that was carried out contrary to the provisions of the LDP and resulted in damages.<sup>94</sup>

## 5.2. Conditions for Liability

There are no significant differences between the Macedonian legislation and the GDPR when it comes to the conditions for liability.

In order for liability to exist, the LDP requires the processing of the data to be contrary to the provisions of the law regulating the obligations of the data processor or controller (Article 101, para. 2). Therefore, any act outside of the limits of the prescribed duties would constitute a wrongful act and give rise to a claim for damages, provided the other conditions are met. This falls within the scope of the (theoretical) understanding of the Law of Obligations, where the wrongful act is defined as act that led to the occurrence of damage, while the damage may be caused by an act or omission or by an object or activity that represents a source of increased risk.<sup>95</sup>

The LDP foresees both the material and the non-material (immaterial) damage as a consequence of the wrongful act. In the Macedonian Tort Law theory, the damage is defined as “[...] any unfavourable result of the wrongful act of a person (tortfeasor) on the property and non-property rights (values) and legally protected interests of a person (injured party) which occurs without his consent (will) and which the tortfeasor is obliged to remove (compensate)”<sup>96</sup>. According to the Macedonian legislation (LOO, Article 142), damage is a reduction of someone's property (ordinary damage) and prevention of its increase (lost profit) as well as violation of personal rights

---

<sup>94</sup> Article 101, para. 4, LDP

<sup>95</sup> Галев Г., Штетно дејствие, Годишник на Правниот факултет „Јустинијан Први во Скопје во чест на Димитар Поп Георгиев, том 40, Правен факултет „Јустинијан Први“ – Скопје, 2006, стр. 42 [Galev G., Wrongful Act, Yearbook of the Iustinianus Primus Law Faculty in Skopje in honor of Dimitar Pop Georgiev, Iustinianus Primus Law Faculty – Skopje, 2006, p. 42]

<sup>96</sup> Галев Г., *Шмета*, Годишник на Правниот факултет „Јустинијан Први во Скопје во чест на Стрезо Стрезовски, том 41, Правен факултет „Јустинијан Први“ – Скопје, 2006, стр. 41 [Galev G., Damage, Yearbook of the Iustinianus Primus Law Faculty in Skopje in honor of Strezovski, Iustinianus Primus Law Faculty – Skopje, 2006, p. 41]



(immaterial damage). Specific for the national legislation is that it provides for the so called 'objective' concept of immaterial damage, defining it as a breach of personal rights rather than subsuming it to its subjective consequences – physical and/or emotional pain and suffering.

The causal link in Macedonian Tort Law also represents the link between the wrongful act and the damage – the damage should be a direct consequence of the wrongful act, and the act itself should be adequate for causing the stated damage.<sup>97</sup> When it comes to obligations grounded on strict liability, as it is the case for those arising from data protection infringements, the existence of a causal link is assumed.<sup>98</sup>

### **5.3. Strict liability for the Data Protection Infringements**

There is nothing in the national law that would lead to any different conclusion than that the liability in the cases of data protection infringements would be strict liability, as discussed above. Article 101, para. 3, LDP provides the ground for the exclusion of liability – when it is proven that the controller or processor is not in any way responsible for the event giving rise to the damage. This position is in line with the general position of the LOO on strict liability; liability will be excluded if the damage is a result of an external act that could not have been foreseen, avoided or removed and attributed to the party (which constitutes *force majeure*<sup>99</sup>) or because of an act of the injured party or a third party.<sup>100</sup>

### **5.4. Assessment of the Damage**

---

<sup>97</sup> Галев Г., *Причинска врска*, Годишник на Правниот факултет „Јустинијан Први во Скопје во чест на Тодорка Оровчанец, том 42, Правен факултет „Јустинијан Први“ – Скопје, 2006, стр. 46 [Galev G., *Damage*, Yearbook of the Iustinianus Primus Law Faculty in Skopje in honor of Todorka Orovchanec, Iustinianus Primus Law Faculty – Skopje, 2006, p. 46]

<sup>98</sup> See Article 159, LOO

<sup>99</sup> Article 126, para. 1, LOO

<sup>100</sup> Article 163, LOO

The national legislation provides for clear rules on the assessment of the damage, both the material and the immaterial. As per Article 178 of the LOO, the injured party has the right to compensation for ordinary damage, as well as for compensation for lost profit. When assessing the amount of the lost profit, the court would take into account the profit that could be reasonably expected according to the regular course of events or according to special circumstances and the realization of which was prevented by the illegal data processing. The issue of liability for immaterial damage and its assessment is more complicated. Immaterial (non-material) damage is compensated immaterially (moral satisfaction) and materially (material satisfaction in the cases provided for in the LOO).<sup>101</sup> The moral satisfaction would consist of actions such as an apology or publication of the verdict<sup>102</sup>. In cases of violation of personal rights, such as the right to data protection, the court, if it finds that the gravity of the violation and the circumstances of the case justify it, will award an equitable monetary compensation, regardless of the compensation of the material damage, as well as in its absence.<sup>103</sup> When deciding on the claim and assessing the damage, LOO provides<sup>104</sup> that the court should take into account “the intensity and duration of the injury that caused physical pain, mental pain and fear, as well as the purpose the compensation serves, but also that the compensation is not contrary to aspirations that are incompatible with its nature and social purpose”. It is to be noted that an act of infringement of the data protection right may constitute a breach of other personal rights, as well as, in particular, the right to privacy, but also honour and reputation. In such cases the court would apply the criteria for the immaterial damage assessment on each instance of a personal data breach.

## 6. Conclusion

The General Data Protection Regulation did introduce substantial changes to the civil liability for a data breach. In comparison with its predecessor - the Data Protection Directive, it increased the emphasis

---

<sup>101</sup> Article 187-a, LOO

<sup>102</sup> Article 188, LOO

<sup>103</sup> Article 189, para. 1, LOO

<sup>104</sup> Article 189, para. 2, LOO

on the liability (and accountability) of the controller, increased the number of direct obligations of the processors and rendered them liable towards data subjects as well, provided for joint and several liability of the controller(s) and processor(s). It also specified the right to compensation for both the material and non-material damage. Keeping in mind its direct effect and applicability, it is expected that there will be no difference in the implementation in the different member states, when it comes to the non-contractual liability for a data breach. However, several questions remain open. First, in the GDPR there is no clear rule as to what constitutes the protected entity – the data subject per se or any natural person that may be affected by a data breach, including a data breach of a third person. Although, we find that the provisions of the GDPR should be interpreted to mean that the specific protection is provided to the data subject, the fact that a third person may be affected indirectly remains. The narrow interpretation does not mean that the third person may not receive protection of their rights at all, but only that it should be done by the general non-contractual liability rules of the member state in question. Still, if the Court of Justice does not provide an opinion on this matter, the national courts of the Member States may apply this provision differently. Second, the GDPR foresees a strict (also called objective) liability for damages, but there is no specific rule that will prevent establishment of fault (intent or negligence) as a ground for liability. Keeping in mind the differences between the two systems, there could be differences in the member states when it comes to the understating and application of the grounds for exclusion or limitation of liability. Last but not the least, the GDPR does not provide any rules for the assessment of the damage and awarding compensation. This may lead to different application in different jurisdictions, especially in those where a *de minimis* rule(s) for damage compensation is applicable.

The Legislation of the Republic of North Macedonia has been approximated with the GDPR. When it comes to the liability for damage the Law on Data Protection proves basic rules of liability, while the Law on Obligations regulates all relevant issues in relation to the exercise of the right to compensation for damages caused by a data protection infringement. A breach of the data protection rights in the national legislation are to be regarded as breach of a personal right. An infringement of the obligations of the controller and/or processor, depending on the circumstances, may also lead to a breach of other

personal rights. So far, there were no civil law actions regarding the protection of this right. Keeping in mind the nature of the right to privacy and its relation to data protection, processing of data contrary to the LDP may lead to an infringement of the right to privacy but also to honour and reputation. Following the strict rules provided in the LOO, the court in this case would assess the damage in relation to breaches of all these personal rights. Still, how the court would act in practice, as well as apply all of the provisions, is yet to be seen.