THE GREAT ESCAPE? LIABILITY OF PUBLIC AUTHORITIES IN THE DATA PROTECTION AREA

Matúš Mesarčík*

Abstract: *The article is focused on the analysis of the liability of public authorities in the data protection area. Public authorities stand outside the spotlight of academics and politics in terms of liability considering the processing of personal data. Nevertheless, public authorities are often controllers of a vast amount of personal data via eGovernment services. Thus, this contribution is aimed to foster the discussion of liability issues concerning public authorities while processing personal data from the point of relevant international data protection legislation and national legislation on the liability of public authorities and its applicability in the data protection area.*

Keywords: *data protection, GDPR, liability, public authorities*

1. INTRODUCTION

Data is the new gold[1] represents one of the biggest leitmotivs of current technological development. The vast amount of data often being qualified as personal data is processed every day by various actors. Non-compliance with data protection law may in some cases trigger related questions of liability.

Although private tech companies are in the spotlight of the media, politicians, and academics, almost no attention is focused on public authorities from the point of liability of data processing.[2] The latter is somehow odd as public authorities are usually one of the biggest personal data controllers in each country taking into account data about citizens. In many cases, data collected and processed by public authorities includes personal data e.g. related to the identity of users of public administration services, sensitive information about health or social security. Additionally, publicly available registers operated by public authorities may contain personal data related to identifiable natural persons that are public officials or in a business relationship with the state.[3]

The aim of the article is thus analysing possibilities of liability for public authorities in the data protection area. The first part of the article focuses on provisions related to liability in general as enshrined in the EU data protection legislation, decision of the Court of Justice of the European Union (CJEU) and soft law provided by the guidelines and opinions of Ar-

* JUDr. Matúš Mesarčík, Ph.D, LL.M, Assistant Professor of Institute of Information Technology Law and Intellectual Property Law, Comenius University in Bratislava, Faculty of Law, Slovak Republic

[1] GODDARD, W. Data – The New Gold Rush for Businesses. In: *IT Chronicles* [online]. 2. 4. 2019 [2020-03-31]. Available at: <https://itchronicles.com/technology/data-the-new-gold-rush-for-businesses/>.

[2] Public authorities are often scrutinized through the lens of surveillance in terms of breaching the right to privacy. VAN DER SLOOT, B. A new approach to the right to privacy or how the European Court of Human Rights embraced the non-domination principle. *Computer Law and Security Review*. 2018, Vol. 34, No. 3, pp. 539–549. NORRIS, C., DE HERT, P., L'HOIRY, X., GALLETA, A. (eds.). *The Unaccountable State of Surveillance. Exercising Access Rights in Europe*. Springer, 2017.

[3] E.g. Register of Public Sector Partners in the Slovak Republic. In: *Ministerstvo spravodlivosti Slovenskej republiky* [online]. [2020-02-28]. Available at <https://rpvs.gov.sk/rpvs>.

ticle 29 Data Protection Working Party (WP29). The second part of the article deals with the public authorities as a specific subject in terms of liability in general and in the data protection area. The third part of the article explores and compares different approaches of holding public authorities liable for damages under specific national laws for breaching data protection regulations[4] and offers a brief analysis of specific aspects of the legislation.

2. LIABILITY AND THE EU DATA PROTECTION AREA

Organizations processing personal data fall under the provisions of EU data protection law represented by the 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 – hereinafter referred to as GDPR).[5] It is of the essence to establish to whom and under what circumstances data protection laws apply.

Historically, requirements of compliance with data protection laws apply to controllers and processors processing[6] personal data[7] about data subjects. Controllers are entities that solely or jointly with others determine purposes and means of the processing of personal data[8] and are primal carriers of responsibility for compliance with data protection rules.[9] The entity is classified as a controller when three elements are fulfilled.[10] Firstly, the controller shall have a determinative influence (or control)[11] over the data processing and this control may stem from explicit legal competence, implicit legal competence or factual influence.[12] Secondly, the controller shall exercise the determinative influence over purposes and means of processing.[13] Thirdly, the influence shall be exercised by one more

[4] This article does not examine the tort law of specific countries in general. Instead, the focus is put on national laws regulating the liability of public authorities without assessing possibilities under traditional tort law before civil courts.

[5] 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. In: *Directive 95/46/EC (General Data Protection Regulation).*OJ L 119, pp. 1–88. 4. 5. 2016.

[6] Processing is defined in Article 4 (2), GDPR in very extensive way as *"any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

[7] Article 4 (1), GDPR defines personal data as *"any information relating to an identified or identifiable natural person."*

[8] Article 4 (7), GDPR.

[9] VAN ALSENOY, B. Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC. *Computer Law and Security Review.* 2012, Vol. 28, No. 1, p. 25.

[10] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor." pp. 7 et seq. 16. 2. 2010.

[11] *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."* pp. 7 et seq.; VAN ALSENOY, B. *Allocating responsibility among controllers, processors, and „everything in between": the definition of actors and roles in Directive 95/46/EC.* p. 30.

[12] Ibid., pp. 10–12.

[13] Although it has to be noted that in some cases the determination of non-essential means of processing may be left to processors. *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."* pp. 14 et seq.

entity classifying as controllers. The institute of joint controllers has emerged during the interpretation of *"jointly"* out of the definition of the controller in Directive 95/46/EC[14] and joint controllers are now explicitly provisioned in the GDPR.

On the other hand, processors process personal data on behalf of controllers.[15] This relationship is best described as a form of delegation where a controller determining the purposes and means of processing outsource processing operations to another entity – processor.

Definitions of controllers and processor changed only slightly during the transition from the Directive 95/46/EC[16] to the GDPR. However, the nature of the liability attributed to these entities shifted during the evolution of the EU data protection laws.

Defining roles and liabilities is often not an easy task. It has to be highlighted that this "binary" setting of the roles of processing operations does not fit the practice in networked environments using new technologies.[17]

2.1 Liability under the Directive 95/46/EC

As an introductory point, it shall be noted that Directive 95/46/EC does not contain specific provisions on the liability of processors. The questions of liability discussed in this part are therefore relevant only to controllers of personal data. Liability in the Directive 95/46/EC is enshrined in Article 23. Article 23 (1) states that *"any person who has suffered damage as a result of an unlawful processing operation or any act incompatible with the national provisions adopted according to this Directive is entitled to receive compensation from the controller for the damage suffered."* The regime is doctrinally characterized as a "strict liability" meaning that the occurrence of the unlawful act is sufficient to claim damages regardless of the intent or fault.[18] In the context of Directive 95/46/EC, the latter is characterized by the fact that the controller is not able to exempt from liability by stating that there have not been "personal fault" or data subject does not have to demonstrate that the unlawful activity has been committed by the controller. The liability in the Directive 95/46/EC is based on the non-delegable duty of care implicating that the controller shall not transfer the liability for breaching data protection laws to a third party (e.g. processor or sub-processor).

In case of a claim for damages, a data subject shall first establish that the entity qualifies as a controller on the merits of the case. Apart from the qualification issues, for the data subject (identified or identifiable natural person) it is of the essence to demonstrate three elements to hold a controller liable for breaching data protection rules: (i) performance of an unlawful act breaching national data protection law implementing the Directive 95/46/EC, (ii) the existence of damages and (iii) causal relationship between unlawful act and the damages incurred.[19]

---

[14] *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."*

[15] Article 4 (8), GDPR.

[16] 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. pp. 31–50. OJ L 281. 23.11.1995.

[17] KUNER, C. *European Data Protection Law – Corporate Compliance and Regulation.* 2nd Edition. New York: Oxford University Press, 2017, p. 72.

[18] VAN ALSENOY, B. Liability under EU Data Protection Law. *JIPITEC.* 2016, Vol. 7, No. 271, p. 273.

[19] Ibid., p. 274.

The controller has only limited options on how to exempt from the liability. Article 23 (2) of the Directive 95/46/EC states 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.* Based on this provision the controller must demonstrate that the unlawful act leading to the damages cannot be attributed to the controller. Recital 55 Directive 95/46/EC clarifies that this is the case when the controller can *"establish fault on the part of the data subject or in case of force majeure."*

Directive 95/46/EC does not contain specific regulation of what type of damages are eligible to the data subjects thus allowing them to claim both material and non-material damages.

As noted at the beginning of the part, Directive 95/46/EC does not impose specific obligations towards processors[20] nor regulate the liability of these entities as such. However, member states could introduce liability of processors in certain cases.[21]

Directive 95/46/EC also latently recognizes the concept of joint controllership.[22] However, the legislation does not allocate the distribution of responsibilities and liability based on the concept. WP29 noted that *"joint control will arise when different parties determine concerning specific processing operations either the purpose or those essential elements of the means which characterize a controller."*[23] The history of the adoption of Directive 95/46/EC suggests[24] that solidary liability is the correct interpretation of the joint controller's regime in the context of liability. On the other hand, WP 29 suggests that solidary liability is not the only option of the liability and allocation of liability may stem from contractual arrangements or factual circumstances.[25] This approach has been doctrinally criticized for vagueness and absence for the clear threshold for join controllership[26] without establishing a *"consistent framework to determine the exact scope and limit of this partial responsibility."*[27]

---

[20] With exception enshrined in the Article 16, Directive 95/46/EC: "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them **except on instructions from the controller**, unless he is required to do so by law."

[21] *"It shall also be considered that, while 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.*" In *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."* p. 28.

[22] See the definition of the controller: "the controller shall mean the natural or legal person, public authority, agency or any other body which **alone or jointly with others determines** the purposes and means of the processing of personal data."

[23] *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."* p. 19.

[24] *"…each of the controllers must be considered as being constrained by the obligations imposed by the Directive to protect the natural persons about whom the data are processed."* COM (95) 375 final – COD287, "Opinion of the Commission under Article 189 b (2) (d) of the EC Treaty, on the European'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.

[25] *Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor."* p. 24.

[26] VAN ALSENOY, B. *Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC.* p. 36.

[27] MAHIEU, R., HOBOKEN VAN, J., ASGHARI, H. Responsibility for Data Protection in a Networked World. On the question of the Controller. "Effective and Complete Protection" and its Application to Data Access Rights in Europe. *JIPITEC.* 2019, Vol. 39, No. 10, p. 45.

To conclude this part, Directive 95/46/EC imposes a strict liability regime on controllers in case of breaching the data protection legislation. This duty cannot be transferred to sub-contractors and may be exempted from only in rather exceptional cases. Directive 95/46/EC does not contain specific provisions on the liability of processors; however, member states may introduce such provisions in their national data protection laws implementing the pertinent directive. The legislation slightly recognizes the concept of joint controllers and in that case, the prevailing interpretation is that joint controllership results in solidary liability.

2.2 Liability under GDPR

Although the origins of data protection law stem from public law, the area of liability (or tort laws) is the dominance of private law.[28] Provisions related to the liability underwent several modifications on their way from the Directive 95/46/EC to GDPR. New data protection legislation contains clarifications essential for the liability in this area. Some authors pointed out that the liability regime according to the GDPR is close to US tort law remedies.[29]

Article 82 (1) GDPR establishes the basis for liability for damages: *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."* Three elements of liability may be derived from the provision: (i) unlawfulness, (ii) damage(s) and (iii) causality.[30] The element of unlawfulness is fulfilled by any infringement of GDPR. In terms of damages, GDPR also explicitly mentions material and non-material damages in the pertinent article. Examples of material damages may include employment dismissal, non-execution of contracts, altering clauses or provisions of contracts based on unlawful processing of personal data. Non-material damages may include negative public exposure, anxiety or discrimination.[31] As a final element of the liability regime in GDPR, the causality between unlawful actions of a competent entity and damages shall exist.[32] When it comes to "who" may claim damages in case of breach of GDPR, the legislation uses the notion of "any person." It seems that the doctrinal interpretation of the term is divided into restrictive and extensive interpretation. The proponents of restrictive interpretation argue that only data subjects may give rise to the pertinent claim. On the other hand, some authors argue the opposite is true and any third party may claim compensation for breach of GDPR.[33] It is agreed with the view that claims from other parties than data subjects may be complicated to succeed due to difficulties in proving damages. However, data protection rules in the EU are aimed to ensure complete and effective pro-

[28] CORDEIRO, A., MENEZES, B. Civil Liability for Processing of Personal Data in the GDPR. *European Data Protection Law Review*. 2019, Vol. 5, No. 4, p. 492.

[29] TRAKMAN, L., WALTERS, R., ZELLER, B. Tort and Data Protection Law: Are There Any Lessons to Be Learnt? *European Data Protection Law Review*. 2019, Vol. 5, No. 4, p. 506.

[30] Ibid., pp. 493–495.

[31] CORDEIRO, A., MENEZES, B. *Civil Liability for Processing of Personal Data in the GDPR*. p. 495.

[32] Article 81 (1), GDPR: *"Any person who has suffered material or non-material damage* ***as a result*** *of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

[33] CORDEIRO, A., MENEZES, B. *Civil Liability for Processing of Personal Data in the GDPR*. pp. 495–496.

tection as it has been enshrined by CJEU in several cases as mentioned throughout this article thus damages shall not be limited only to data subjects.

2.2.1 Controllers and liability

As an introductory note, it shall be noted that a "strict" liability regime remains applicable to controllers. The latter is confirmed by Article 82 (2) GDPR: *"Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation."* It is important to highlight that the GDPR strengthens the principle of accountability.[34] This principle in sum requires controllers to demonstrate compliance with the regulation in two ways. First by fulfilling more formal obligations e.g. maintain records of processing of personal data, drafting and publishing privacy policy or internal data protection documentation (security policy or internal data protection policy). Secondly by implementing appropriate organizational and technical measures into data protection practice e.g. identity management, procedures for notification of personal data breaches or introducing a different level of access to personal data for specific employees.[35] The aforementioned in practice might mean that when data subject offers the evidence of unlawful processing activity, the burden of proof is shifted towards the controller to demonstrate compliance with GDPR.[36]

The controller may escape liability only in case of "events beyond control." Article 82 (3) GDPR stipulates that *"A controller….shall be exempt from liability…if it proves that it is not in any way responsible for the event giving rise to the damage."* Some authors even suggest that the wording "in any way" represents tightening the exception.[37] The important development of liability clauses in the data protection areas is also characterized by explicit recognition of liability exceptions based on the so-called eCommerce Directive[38] in Article 2 (4) GDPR.[39] In practice, this recognition is essential as some authors emphasize the need for a more uniform approach to the issue promoting legal certainty.[40]

2.2.2 Processors and liability

Though specific obligations and liability of processors are not presented in the Directive 95/46/EC, EU legislators took the step forward and regulated the issue in GDPR. Obliga-

[34] Article 5 (2), GDPR.

[35] VAN ALSENOY, B., DUMORTIER, J. The accountability principle in data protection regulation: origin, development and future directions. In: D. Guagnin et al. (eds.). *Managing Privacy Through Accountability*. Palgrave Macmillian, 2012, pp. 49–82.

[36] VAN ALSENOY, B. *Liability under EU Data Protection Law*. p. 283.

[37] LAROUCHE, P., PEITZ, M. PURTOVA, N. Consumer Privacy in network industries – A CERRE Policy Report. *Centre on Regulation in Europe*. 2016, p. 58.

[38] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market ('Directive on electronic commerce'). OJ L 178. pp. 1–16. 17. 7. 2000.

[39] *"This 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."*

[40] CUNHA, M., AZAVEDO, V. et. al. Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. *International Data Privacy Law*. 2002, Vol. 2, No. 2, p. 57.

tions for the processor may stem directly from GDPR[41] or from the contract concluded with the controller in compliance with Article 28 (3) GDPR. As per the fact that the processor always acts on behalf of the controller, deviating from the lawful instructions of the controller or data processing agreement form the background for liability of processors.

The legislation provisions a proportional liability regime for processing operations where a processor is involved. This conclusion arises from Article 82 (2) GDPR: *"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."* However, GDPR provides the option for the processor to be held liable for *"the entire damage in order to ensure effective compensation of the data subject."*[42] It shall be noted that mere involvement of the processor in the processing of personal data shall not mean that a processor may be held liable for wholly or partially for the damage.[43] Damage may be attributed to the processor only under the condition that the processor's activities during the processing of personal data caused damage and actions related to the damages were either contrary to the obligations under the GDPR or controller's instructions. If this is the case, the processor may be held liable for damages. On the other hand, GDPR does not contain any threshold when it comes to the degree of responsibility therefore in theory the processor may be held liable for the whole amount of the damage.[44] From the point of view of the data subject, he/she has a choice who to sue in situations where processing operations are carried out by the controller and (at least partly) by processors.[45] What is more, the controller has an option to redress – compensation from the processor if it is established that the processor was in breach of GDPR or act out of the scope of the controller's instructions.[46]

In terms of defenses and type of eligible damages, the same rules as for the controllers apply.

2.2.3 Joint controllers and liability

GDPR explicitly recognizes the concept of joint controllers.[47] Joint controllers shall determine their responsibilities concerning compliance with GDPR in a transparent manner. In terms of liability, it shall be highlighted that based on the wording of GDPR every joint controller may be held liable for the damage in the entirety. It is worth noting that Article

[41] E.g. obligation to maintain records of processing activities based on the Article 30 GDPR, notification obligation about the personal data breach to the controller according to the Article 33 (2) GDPR or appointment of data protection officer per Article 37 GDPR.

[42] Article 82 (4) GDPR.

[43] VAN ALSENOY, B. *Liability under EU Data Protection Law*. p. 285.

[44] Ibid., supra note 108.

[45] Article 82 (4), GDPR: *"Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject."*

[46] Article 82 (5), GDPR.

[47] Article 26 (1), GDPR: *"Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."*

83 GDPR does not contain specific rules on allocating fines among joint controllers in case of breach of GDPR. Defenses and liability exceptions apply accordingly as in the case of controller and processors.

Joint controllership and joint liability issues have been under the scrutiny of the Court of Justice of the European Union (CJEU) recently in cases *Wirtschaftsakademie* and *Fashion ID* following the basic premise established by *Google Spain*. In the case of *Google Spain*[48] the Luxemburg court noted towards the data protection issues (including liability) of search engine and original publisher of news that: *"…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."*[49] CJEU emphasized that meeting data protection obligations shall be analyzed through the lens of the "powers and capabilities" of the controller. Although the case concerns specific entity processing personal data (search engine), the CJEU seems to allow interpretation of responsibilities in an exceptional manner opening the door for avoiding liability.

Wirtschaftsakademie[50] concerned operating a fan page on Facebook and correct classification of the provider of the social network (Facebook) and operator of the fan page (Wirtschaftsakademie). The cornerstone of the deliberation of the court was to establish whether and to what extent the operator of the fan page determine purposes and means of the processing of personal data jointly with Facebook. The Luxembourg court noted in the beginning of the judgment, that although not every user of Facebook shall automatically be considered as a controller, the specific situation of the operator of fan page derives from the fact that *"by creating such a page, allows Facebook to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account."*[51] CJEU also noted that the operator of the fan page has a margin of appreciation as to the determination of targeting filters (selecting audience) and criteria for how the statistics are created.[52] Based on these conclusions the court established that Facebook and the operator of a fan page are joint controllers. However, CJEU highlighted the importance of analyzing the state of processing as different controllers may be involved in various stages on the various level, therefore *"the level of responsibility of each of them must be assessed concerning all the relevant circumstances of the particular case."*[53] Doctrine characterized the decision as to the switch from macroscopic to microscopic view on the processing of personal data.[54] However, the court still did not address some of the

[48] Decision of the CJEU from 13 May 2014, Google Spain SL a Google Inc. v Agencia Española de Protección de Datos (AEPD) a Mario Costeja González. Case n. C-131/12.

[49] Ibid., para 38.

[50] Decision of the CJEU from 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH. Case n. , C 210/16.

[51] Ibid., para 35.

[52] Ibid., para 36.

[53] Ibid., para 43.

[54] MAHIEU, R., HOBOKEN VAN, J., ASGHARI, H. *Responsibility for Data Protection in a Networked World. On the question of the Controller. "Effective and Complete Protection" and its Application to Data Access Rights in Europe.* p. 48.

crucial considerations of joint controllership like mechanisms for allocating responsibilities or the relationship between determining purposes *and* means of processing.[55]

A similar outcome lies within the conclusions of the *Fashion ID* case.[56] The dispute involved a situation where a web page provider (Fashion ID – online clothing retailer) embedded on its website the 'Like' social plugin from the social network Facebook. The issue at question was that every time a visitor visits the web page of the online clothing retailer the web transmits data about visitors to Facebook regardless of the existence of the account on the social network. The Court again acknowledged the broad interpretation of the notion of controller following the decision in *Wirtschaftsakademie.* Joint determination of purposes and means have been found at the origin of processing operations (collection and disclosure).[57] Different liability may be attributed to various actors in personal data processing taking into account different stages of processing.[58]

Both of the aforementioned decisions reflect the complexity of the correct determination of entities in light of the personal scope of GDPR. What is more, CJEU applies the principle of "effective and complete protection"[59] in light of fundamental rights and freedoms, therefore, aiming to ensure the protection of all potential data subjects affected by the processing of personal data by various parties.

3. LIABILITY OF PUBLIC AUTHORITIES IN THE DATA PROTECTION AREA

This section of the article focuses on the liability issues related to public authorities especially in terms of the data protection area. First, the introductory notes are made towards the specific status of public authorities in terms of liability. Second, both Directive 95/46/EC and GDPR are assessed if any exception(s) to public authorities apply during the processing of personal data. Finally, the brief analysis of Slovak and Austrian public authorities liability laws are made and partial conclusions are offered.

3.1 General remarks towards the liability of public authorities

The liability of public authorities, in general, serves as a great example of a complex regulatory issue in the current era. Though much academic and legislative attention is paid to formulating common principles of tort laws in terms of private entities[60] liability of public authorities did not receive much political or academic attention.

However, the situation has changed in recent years. First, the European Group on Tort Law that has drafted a collection of Principles of European Tort Law (PETL) decided to

[55] Ibid., p. 49.

[56] The decision of the CJEU from 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. Case n. C 40/17.

[57] Ibid., paras 79-81.

[58] Ibid., para 71.

[59] MAHIEU, R., HOBOKEN VAN, J., ASGHARI, H. *Responsibility for Data Protection in a Networked World. On the question of the Controller. "Effective and Complete Protection" and its Application to Data Access Rights in Europe.* pp. 40–41.

[60] See e.g. projects pursued by European Group on Tort Law. In: *European Group on Tort Law* [online]. [2020-03-31]. Available at: <http://www.egtl.org/index.html>.

put more focus on the issue of liability of public authorities.[61] The expert group on the liability of public authorities has been formed due to three reasons: (i) emergence of national legislation regulating the liability of public authorities within respective EU member states, (ii) judicial recognition of liability of EU member states for breaching the EU law and (iii) exclusion of public authorities from PETL.[62]

Secondly, academics attempted to provide the expert audience with comprehensive studies devoted to the national laws on the liability of public authorities or comparative studies.[63]

European Group on Tort Law in PETL decided to exclude public authorities from the scope of the principles. The exception is based on the fact that many national countries adopted specific legislation covering the area influenced by historical and cultural developments.[64] What is more, commentators state that specific regulation by PETL would interfere with administrative law in a more than anticipated way.[65]

A similar conclusion has been made by the European law of tort in Book IV of the Draft Common Frame of Reference (DCFR).[66] Provisions under the heading "Non-contractual liability arising out of damage caused to another" explicitly exclude public authorities from the application: *"This Book does not govern the liability of a person or body arising from the exercise or omission to exercise public law functions or from performing duties during court proceedings."*[67]

The reluctance of expert groups formulating common framework in the tort law area stems mainly due to specific status and tasks endowed to public authorities and the existence of various legislation across the EU reflecting the specifics of each country.

Public authorities operate for the general interest of public good. Unlike private entities, public authorities aim to provide sound administration and public services for the benefit of everyone. It shall be noted that the provision of many services moved from the offline environment to online space and public services are in many countries provided elec-

[61] Mainly by meetings of the group devoted to the liability of public authorities as seen in the publicly and by publishing extensive comparative study as the outcome of these meetings. See Meetings of the European Group on Tort Law. In: *European Group on Tort Law* [online]. [2020-03-31]. Available at: <http://www.egtl.org/meetings.html>. OLIPHANT, K. (ed.). *The Liability of Public Authorities in Comparative Perspective*. 1st Edition. Cambridge: Intersentia Ltd., 2016.

[62] OLIPHANT, K. Formulating Common Principles of Public Authority Liability Law. In: P. Mankowski – W. Wurmnest (eds.). *Festschrift für Ulrich Magnus*. München, 2014, pp. 97–98.

[63] OLIPHANT, K. (ed.). *The Liability of Public Authorities in Comparative Perspective*; OLIPHANT, K. *Formulating Common Principles of Public Authority Liability Law*; OLIPHANT, K. Comparative Remarks. In: H. Koziol – B. Steininger (eds.). *European Tort Law*. Vienna: Springer-Verlag, 2018; BELL, J., BRADLEY, A. (eds.). *Governmental Liability: A comparative survey*. London: UKNCCL, 1991; MARKESINIS, B. et al. *Tortious Liability of Statutory Bodies*. Oxford: Hart Publishing, 1999; FAIRGRIEVE, D. et al. (eds.). *Tort Liability of Public Authorities in Comparative Perspective*. London: BIICL, 2002; VAN DAM, C. *European Tort Law*. 2nd Edition. Oxford: Oxford University Press, 2013.

[64] EUROPEAN GROUP ON TORT LAW. *Principles of European Tort Law Text and Commentary*. Vienna: Springer-Verlag, 2005, p. 119.

[65] Ibid., p. 113.

[66] The document has been prepared by STUDY GROUP ON EUROPEAN CIVIL CODE / RESEARCH GROUP ON EC PRIVATE LAW (ACQUIS GROUP). Principles, Definitions and Model Rules of European Private Law. In: *K. U. Leuven* [online]. 2009 [2020-03-31]. Available at: <https://www.law.kuleuven.be/personal/mstorme/2009_02_DCFR_OutlineEdition.pdf>.

[67] Article VI. – 7:103: Public law functions and court proceedings, DCFR.

tronically causing new challenges of the regulatory framework.[68] What is more, these services have to be delivered efficiently to fulfill their purpose.

Public authorities are granted with a range of powers much different from the position of private companies. From the other point of view, citizens seem particularly vulnerable compared to the strong position and powers of public authorities e.g. in terms of surveillance or enforcement in general. Further uniqueness related to the status of public authorities stems from financing as these entities are funded by public funds and their accountability via the political process.[69]

The second specific is that in terms of liability of public authorities, a clear connection towards the principle of separation of power has to be made. Van Dame states that taking into account peculiarities of this principle in many legal systems the justifiability of claims brought against public authorities has to be set by the executive branch of power making the judiciary potentially unprepared to hear such claims.[70]

The third specific relates to the case when damage is successfully claimed by a person as damages are paid from "taxpayers' money."[71] This is the crucial point when it comes to the debate about the liability of public authorities as damages have to be covered from the public purse and might miss forming the national budget.

As highlighted above, many countries introduced regulation of liability of public authorities within their legal systems. However, these rules differ from country to country as per legal traditions and culture. Three types of regulatory approaches presented in the European jurisdictions may be emphasized. The first approach called *the public law model* consists of special laws adopted to regulate the liability of public authorities and this law is applied by administrative courts. This model is represented by the legal systems of France[72] and partially Slovakia and the Czech Republic. The second regulatory approach named the *private law model* is represented by the situation when the liability of public authority is governed by civil law rules on tort and applied by civil courts. This is the case in Belgium.[73] The third regime is *hybrid* and relates to a situation where civil courts apply provisions of civil law that imposes liability for public servants in terms of breach of their official duty and then rely on constitutional provisions allowing to transfer the liability from public servant to the state. This regime applies to Germany.[74]

To conclude general remarks in terms of liability of public authorities, two important highlights have to be made. First, specific status and tasks delegated upon public authorities ignited the debate about special regulation of liability for these entities in many EU

[68] ANDRAŠKO, J. Exercise of Public authority in electronic form. Warszawa: Administracja publiczna a gospodarka, Ius Publicum, 2018, pp. 333-349; SOPÚCHOVÁ-RALBOVSKÁ, S. Information systems as essential prerequisites for electronization of public administration. *CER Comparative European research*. 2017, No. 2, pp. 121–124.

[69] OLIPHANT, K. *Formulating Common Principles of Public Authority Liability Law*. p. 100; VAN DAM, C. *European Tort Law*. pp. 577–578.

[70] VAN DAM, C. *European Tort Law*. p. 531.

[71] Ibid.

[72] See e.g. comprehensive comparison of British and French approach in: FAIRGRIEVE, D. *State Liability in Tort: A Comparative Law Study*. Oxford: OUP, 2013.

[73] OLIPHANT, K. *Formulating Common Principles of Public Authority Liability Law*. p. 100; VAN DAM, C. *European Tort Law*. p. 99.

[74] Ibid.

jurisdictions. Second, as a result, many EU member states adopted legislating provisioning liability of public authorities. Though models of legislation concerning the liability of public authorities may differ, the legislation aims to tackle the specifics of the issue.

3.2 Liability of public authorities in the data protection area

Although data protection area is neutral from the point of "who" is processing personal data (if the entity qualifies as a controller or processor, the legislation applies regardless the public or private status of the entity), several tendencies may be observed from the development of data protection law in Europe.

First data protection act was adopted in 1970 in German state of Hessen.[75] The law has been adopted to regulate personal data processing by governmental authorities.[76] The same conclusion shall be made towards the German Federal Data Protection Act from 1977.[77] Subsequently, the first Swedish Data Protection Act from 1973 (*Datalog*)[78] did not contain specific regulation of data processing activities by public authorities. This was subject to the specific supplementary laws in Sweden.[79]

The Organisation for Economic Co-operation and Development (OECD) issued in 1980 its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Guidelines).[80] The guidelines represent the first comprehensive international instrument related to the processing of personal data although the non-binding nature of the guidelines shall be emphasized. Based on Article 2 *"These Guidelines apply to personal data, whether in the* ***public*** *or private sectors, which, because of how they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."* This is confirmed by § 44 of the Explanatory report.[81] Furthermore, the Explanatory report adds that the data controller may be *"legal or natural person,* ***public authority****, agency or any other body."*[82] However, Article 19 of the Guidelines provisioning requirement

[75] Datenschutzgesetz (GVBl. II 300-10) vom 12. Oktober 1970. In Gesetz- und Verordnungsblatt für das Land Hessen. 1970 Nr. 41, S. 62. 12. 10. 1970. In: *Landtagsinformationssystem* [online]. [2020-03-31]. Available at: <http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1>.

[76] OOSTVEEN, M. The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? In: M. Bakhoum et al. (eds.). *Personal Data in Competition, Consumer Protection, and Intellectual Property Law. Towards a Holistic Approach*. Vienna: Springer-Verlag, 2018, p. 32 et seq.

[77] RICCARDI, J. L. The German Federal Data Protection Act of 1977: Protecting the Right to Privacy? *B.C. Int'l & Comp. L. Rev*. 1983, Vol. 6, No. 243.

[78] Datalog given in the Palace of Stockholm, May 11, 1973, SFS 1973:289.

[79] ÖMAN, S. Implementing Data Protection in Law. In: *Stockholm Institute for Scandinavian Law* [online]. 2010 [2020-03-31]. Available at: <https://www.scandinavianlaw.se/pdf/47-18.pdf>. p. 390.

[80] OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In: *OECD* [online]. [2020-03-31]. Available at: <https://www.oecd.org/internet/economy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[81] *"As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the* ***public sector****. These notions may be defined differently by different Member countries."*

[82] § 40, Explanatory Report to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In: *OECD* [online]. [2020-03-31]. Available at: <https://www.oecd.org/internet/economy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

of national implementation opens the possibility to regulate control mechanisms related to public authorities in line with national legal culture and traditions.[83] These public authority aspects remain unchanged in the revised version of the Guidelines from 2013.[84]

Again in 1981, the Council of Europe adopted the first legally binding international document on the processing of personal data – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data commonly referred to as Convention 108. The purpose of the Convention 108 is *"to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him."*[85] As in the OECD Guidelines, Convention 108 applies to both private and public sectors[86] and public authorities may qualify as controllers of personal data.[87] The reason for the inclusion of public authorities within the scope of the Convention 108 is further explained in the Explanatory Memorandum to the Convention 108: *"First, Article 3 imposes obligations on the Member States to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country. The distinction public sector/private sector is not found in the other provisions of the convention, especially since these terms may have a different meaning in different countries. But it may play a role in the declarations which the Parties may make with regard to the scope of the convention."*[88] In the Modernized version of the Convention 108 from 2018[89] public authorities were added as possible entities qualifying for recipients and processors[90] as legal definitions of recipients and processors are not included in the original version of the document from 1981.

In terms of public authorities, Directive 95/46/EC provides that these entities may qualify for controllers,[91] processors,[92] third parties[93] or recipients[94] implying the application of the law in the public sector. This is also concludingly confirmed by the scope of the Directive 95/46/EC itself deriving from Article 1[95] that does not make the difference between

[83] This is confirmed by § 69 of Explanatory Report: *"The opening sentence shows the different approaches which might be taken by countries, both generally and concerning control mechanisms (e.g. specially set up supervisory bodies, existing control facilities such as courts,* ***public authorities,*** *etc.)."*

[84] OECD. OECD Privacy Framework. In: *OECD* [online]. 2013 [2020-03-31]. Available at: <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[85] Article 1, Convention 108.

[86] Article 3 (1), Convention 108 reads: "The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors."

[87] Article 2 (d), Convention 108.

[88] § 33, Explanatory Memorandum to the Convention 108.

[89] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. In: *Council of Europe* [online]. 18. 5. 2018 [2020-03-31]. Available at: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf>.

[90] Article 2 (e) and (f), Convention 108.

[91] Article 2 (d), Directive 95/46/EC.

[92] Article 2 (e), Directive 95/46/EC.

[93] Article 2 (f), Directive 95/46/EC.

[94] Article 2 (g), Directive 95/46/EC.

[95] "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

the processing of personal data in the private or public sector. In terms of liability, no special attention is paid to public authorities.

The latter is changed in GDPR. Public authorities are frequently mentioned in the introductory parts of the regulation.[96] As in Directive 95/46/EC, public authorities may qualify as controllers,[97] processors,[98] third parties[99] or recipients[100] under the GDPR. Public authorities are excluded from using the legal ground of legitimate interest in the processing operations carried out within the performance of their tasks.[101] Furthermore, public authorities are excluded[102] from the obligation to designate a representative in the European Union in case of extraterritorial applicability of GDPR.[103] On the other hand, public authorities are under the obligation to appoint a data protection officer under Article 37 (1) (c) GDPR. No monitoring body is required where the code of conduct is established and used by public authorities.[104]

However, GDPR introduces a specific exception when it comes to the liability of public authority considering imposing administrative fines. GDPR provides two levels of administrative fines. The decisive factor when assessing what set of fines to use is the severity of breach explicitly stated in accompanying sections of Article 83 GDPR. First set of 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. The second set of administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher is designated for the infringements of e.g. basic principles of processing as per Article 5 GDPR, data subject rights or cross-border transfer of personal data to third countries.[105]

Article 83 (7) GDPR is devoted to public authorities considering imposing administrative fines on them. This article reads: *"Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2),* ***each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State****."* This in practice means that member states were allowed to exclude the possibility of fining public authorities based on the violations

[96] See e.g. Recital 6, Recital 7, Recital 19, Recital 31, Recital 43, Recital 45, Recital 47, Recital 49, Recital 80, Recital 92 or Recital 93 of GDPR.
[97] Article 4 (7), GDPR.
[98] Article 4 (8), GDPR.
[99] Article 4 (10), GDPR.
[100] Article 4 (9), GDPR.
[101] Article 6 (1), last sentence.
[102] From Article 27 (2) (b), GDPR.
[103] Article 3 (2), GDPR reads: *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
(b) the monitoring of their behavior as far as their behavior takes place within the Union."
[104] Article 41 (6), GDPR.
[105] MESARČÍK, M. *Nová právna úprava správneho trestania.* Bratislava: Univerzita Komenského, Právnická fakulta, 2017, pp. 83–90.

of GDPR. The provision is further explained on the example of Denmark and Estonia in Recital 151: *"The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia, the fine is imposed by the supervisory authority in the framework of a misdemeanor procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities."*The exception has been added during the legislative process and is absent in the original proposal of GDPR prepared by the European Commission. Discussed provision was added during the first reading by the Council.[106]

The pertinent exception has been seized by many member states some of them entirely excluding public authorities from fining them or introducing specifying conditions and limitations in terms of fines for them. Three categories of countries may be derived based upon (not) seizing the exception in Article 83 (7).[107] The first group is represented by member states that do not introduce any limitations on public authorities in terms of administrative fines. The second group of countries is represented by member states that exclude public authorities from fining entirely. The third group of member states provisioned specific limitations and conditions upon which public authorities may be fined (e.g. via the maximum amount of fine or as per specific actions performed by public authorities – offering goods or services).

Possibility of fining public authorities	EU Member States
No limitations	Bulgaria, Iceland, Italy, Latvia, Netherlands, Portugal, Slovakia, Spain, United Kingdom
Public authorities entirely excluded	Austria, Croatia, Estonia, Finland, France Germany, Liechtenstein, Luxembourg
Specific conditions and limitations	Belgium, Denmark, Cyprus, Czech Republic, Greece, Hungary, Ireland, Lithuania, Malta, Poland, Romania, Slovenia, Sweden

Figure 1: *Overview of liability of public authorities for breaching GDPR in the EU*

From the point of legal theory, liability is bearing consequences for non-compliance with legal norms.[108] Legal liability stands on imposing sanctions prescribed by law and

[106] Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and repealing Directive 95/46/EC – Draft Statement of the Council's reasons, 2012/0011 (COD). p. 33.

[107] Sources include respective national data protection acts, GDPR EU Countries. In: *Alston & Bird* [online]. [2020-03-31]. Available at: <https://www.alston.com/files/Uploads/gdprtracker/assets/gdpr-eu-countries.pdf>; GDPR National Implementation. In: *White & Case* [online]. [2020-03-31]. Available at: <https://www.whitecase.com/publications/article/gdpr-guide-national-implementation>.

[108] FÁBRY, B., KASINEC, R., TURČAN, M. *Teória práva.* 1st Edition. Wolters Kluwer, 2017, p. 219.

suffering this harm on the side of the perpetrator.[109] The purpose of the legal liability is to rectify and eliminate the consequences caused by illegal behavior setting the compliant status with law.[110]

It seems that punishing public authorities in the data protection area is extremely limited in the countries that exclude these entities from the scope of fining.

It is argued that the specific position of public authorities as enshrined in the literature[111] does not stand in the data protection area. First, the specific nature of the entity is irrelevant as per the fact that GDPR applies to any entity processing personal data regardless of the private or public nature of the controller or processor. Secondly, it is undisputed that public authorities provide crucial public administration services for citizens and this activity encompasses a vast amount of personal data. Therefore, it is our opinion that taking due account of providing these services public authorities shall be liable and sanctionable to the full extent. What is more, there are numerous cases of fines for breaching GDPR for public authorities in countries where public authorities are fully or partially liable. The highest fine imposed in Bulgaria was 2,600,000 € to the National Revenue Agency.[112] In Slovakia, the highest fine amounts to 50 000 € and was imposed on Social Insurance Agency.[113] Fines were also imposed on public hospitals in Portugal,[114] the Netherlands,[115] and Cyprus.[116] Belgian data protection authority imposed fines on several mayors[117] and the same authority was fined in Hungary[118] and Poland.[119] Land authority was found to be in breach of GDPR and fined in Malta.[120]

---

[109] Ibid.

[110] BREJCHA, A. *Odpovědnost v soukromém a veřejném právu.* 1st Edition. Praha: CODEX Bohemia, 2000, p. 21.

[111] See part 3.1 of this article.

[112] Информация за извършена проверка в Националната агенция за приходите. In: *Republic of Bulgaria Commission for Personal Data Protection* [online]. 29. 8. 2019 [2020-03-31]. Available at: <https://www.cpdp.bg/index.php?p=news_view&aid=1519>.

[113] NEJEDLÝ, T. Sociálna poisťovňa porušila GDPR. In: *Trend* [online]. 13. 11. 2019 [2020-03-31]. Available at: <https://www.etrend.sk/ekonomika/socialna-poistovna-porusila-gdpr-pokutu-50-tisic-eur-nechce-zaplatit.html>.

[114] The decision of Portugal DPA. In: *CNPD* [online]. [2020-03-31]. Available at: <https://www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf>.

[115] Haga beboet voor onvoldoende interne beveiliging patiëntendossiers. In: *Autoriteit Persoonsgegevens* [online]. 16. 7. 2019 [2020-03-31]. Available at: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers>.

[116] Cyprus GDPR Commissioner fines newspaper and hospital. In: *AGP* [online]. 1. 3. 2019 [2020-03-31]. Available at: <https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/ >.

[117] L'Autorité de protection des données prononce une sanction dans le cadre d'une campagne électorale. In: *Autorité de protection des données* [online]. [2020-03-31]. Available at: <https://www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-prononce-une-sanction-dans-le-cadre-dune-campagne>; and La Chambre Contentieuse sanctionne deux candidats aux élections communales de 2018. In: *Autorité de protection des données* [online]. [2020-03-31]. Available at: <https://www.autoriteprotectiondonnees.be/news/la-chambre-contentieuse-sanctionne-deux-candidats-aux-elections-communales-de-2018>.

[118] Hungary's data protection authority levies two EUR 3100 fines for privacy violation. In: *CMS* [online]. 29. 3. 2019 [2020-03-31]. Available at: <http://www.cms-lawnow.com/ealerts/2019/03/hungarys-data-protection-authority-levies-two-eur-3100-fines-for-privacy-violations?cc_lang=en>.

[119] The decision of Polish DPA. In: *Urząd Ochrony Danych Osobowych* [online]. 18. 10. 2019 [2020-03-31]. Available at: <https://uodo.gov.pl/decyzje/ZSPU.421.3.2019>.

[120] IDPC fines lands authority data breach. In: *GVZH Advocates* [online]. [2020-03-31]. Available at: <https://www.gvzh.com.mt/malta-news/idpc-fines-lands-authority-data-breach/>.

The third specific of public authorities oscillates about funding from public resources and paying potential damage from the same source. It is of the essence to note that public authorities may be seen as standards of compliance with norms adopted or recognized by the state. In case that public authority causes damage within the exercise of the official authority, then taxpayers have the full right to have information about the case and reflect it via mechanisms available in a democracy (for example elections).

However, many EU countries introduced specific laws on the liability of public authorities as discussed above and it is of the essence to examine if these laws are suitable as a substitute for imposing fine by data protection authorities and enforce damages by natural or legal persons.

3.3 Damage caused by public authorities in the data protection area and regulatory challenges

In this part of the article two jurisdictions are examined from the point of liability of public authorities in the data protection area – Slovakia and Austria. Slovakia is one of the countries where imposing administrative fines on public authorities is allowed in full and no exceptions or limitations apply. The liability of public authorities is regulated by Act on Liability of Public Authorities (hereinafter referred to as the Slovak Act on Liability of Public Authorities).[121] On the other hand, the Austrian legislator decided to seize the open clause in Article 83 (7) GDPR and excluded public authorities from being fined based on GDPR. The liability of public authorities in Austria is regulated by so-called *Amtshafttungsgesetz* (hereinafter referred to as AHG).[122] It is of the essence to briefly compare respective laws on public authorities and derive regulatory challenges with a focus on the data protection area.

As an introductory point, it shall be noted that GDPR and special national laws regulating the liability of public authorities differ on the point of aim of the legislation. GDPR aims to establish rules for the protection of natural persons concerning the processing of personal data and rules relating to the free movement of personal data[123] and enhance the protection of fundamental rights and freedoms especially right to data protection.[124] The free movement of personal data within the EU is guaranteed by the regulation.[125] Supervisory authorities may impose administrative fines or other appropriate coercive mechanisms when obligations in GDPR are breached or ought to be breached.[126] As mentioned above, the GDPR reflects a strict liability regime for controllers and processors. Possibility

[121] Act no. 514/2003 on Liability for Damage Caused in the Context of Exercise of Public Authority (*Zákon o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a zmene niektorých zákonov)*.

[122] Federal Act on the Liability of Territorial Authorities and other Bodies and Institutions of Public Law for Damage caused when Implementing the Law (Liability of Public Bodies Act – AHG): BGBl. Nr. 20/1949 idF.

[123] Article 1 (1), GDPR.

[124] Article 1 (2), GDPR.

[125] Article 1 (3), GDPR.

[126] Article 29 Data Protection Working Party Guidelines on the application and setting of administrative fines for the Regulation 2016/679. Adopted on 3 October 2017, p. 5.

to claim damages on the side of data subjects enshrined in Article 82 may be seen as "a second step" as a breach of GDPR is required as a prerequisite for a successful claim for damages by the injured party. Furthermore, these cases are not decided by supervisory authorities but respective courts usually within the national limits of tort laws. When it comes to liability of public authorities for damages, specific national laws are introduced to hold public authorities liable and compensate injured parties.[127] In comparison, GDPR sets forth rules concerning the processing of personal data in general with enforcement mechanisms. The aim of the legislation is thus different and has to be taken into account.

Considering discussed jurisdictions, three aspects must be analyzed in terms of claiming damages arising in the data protection area using special laws focused on the liability of public authorities.

The first potential obstacle may lie in the limited application of national laws on the liability of public authority. This means that not every public authority in a specific country may be held liable for damages as some are explicitly excluded by legislation or laws are restrictive in terms of scope. Slovak Act on Liability of Public Authorities applies only to unlawful decisions of public authorities and improper official procedures. Although definitions of these notions are absent, common interpretations of these notions may set the threshold too high to be applied in the data protection area. As an illustration, there may be the case when public authority does not implement appropriate organizational and technical measures in line with GDPR and processing of personal data leads to the personal data breach in the form of the personal data leak. In the words of the Slovak Act on Liability of Public Authorities, this case shall not be classified as having unlawful decisions in place since no decision had been as presumed by the legislation. The argument of improper official procedure may be more valid although the demonstrative list[128] of what belongs under the notion of improper official procedure highlights the issue of competence and its limits during the procedure towards the individual. Compliance with GDPR is not the issue of competence of any entity but rather a legal obligation to protect rights and freedoms. However, the vagueness of the definition opens the possibility of enforcing damages in the data protection area from public authorities although this has never been tested in practice. On the other hand, Austrian AHG seems to apply a more dynamic approach when defining when the public authority liability may be attributed to the specific entity. AHG requires any unlawful act of persons at fault when implementing the law on behalf of legal entities prescribed by the law. Such a broad definition of actions or omissions that may attract the liability regime may just fall within boundaries of compliance with GDPR. Obligations enshrined in GDPR for controllers and processors require imple-

[127] See § 1 (1) AHG and § 1 Slovak Act on Liability of Public Authorities.

[128] The legislation provides a demonstrative set of categories that may fall within the notion of improper official procedure specifically breach of the obligation of a public authority to take action or make a decision within a statutory period, failure of a public authority to exercise public authority, unnecessary delays in proceedings or other unlawful interference with rights, legally protected interests of natural persons and legal entities; the procedure or the result of the procedure of the National Council of the Slovak Republic in the exercise of its competence under Art. 86 a) and d) of the Constitution of the Slovak Republic and the procedure or outcome of the procedure of the Government of the Slovak Republic in the exercise of its competence under Art. 119 b) of the Constitution of the Slovak Republic. § í (1), Slovak Act on Liability of Public Authorities.

mentation and non-compliance with data protection rules may amount to unlawfulness as this is the prerequisite of liability in Article 82 (1). As it is seen from the different scopes of public authority liability laws in Slovakia and Austria, triggering the liability regime may be a difficult task.

Secondly, both discussed acts relate to the exercise of public authority. However, it is not clear what amounts to the exercise of public authority and doctrinal interpretation differs from country to country. Specifically, the question is whether (non)-compliance with legal obligations (in this case prescribed by GDPR) may qualify as the exercise of public authority. It is of the opinion of the author that exercise of public authority has to be connected to some specific task or another obligation involving the processing of personal data prescribed by law as the exercise of public authority. Illustratively, public authorities often offer electronic services of public administration (eGovernment) based on laws. The provision of electronic services of public administration involves the processing of personal data of users and amounts to the exercise of public authority at the same time. In case of breach of GDPR e.g. in the form of a personal data breach within the provision of electronic services of public administration, this situation shall be assessed as potential faulty conduct by the public authority during the exercise of public authority by not implementing requirements prescribed by GDPR during the provision of public services in electronic form. However, the applicability of this construct shall be tested in practice.

Thirdly, the question of damage has to be carefully assessed. Both, Slovak Act on Liability of Public Authorities and Austrian AHG requires harm as an element of the successful claim, therefore, it is crucial for data subject to prove that by the violation of GDPR he has suffered damage. Recital 75 GDPR lists examples of situations how material and non-material damages may occur. The recital mentions identity thefts, financial damage in form of loss, loss of reputation, discrimination, loss of confidentiality provisioned by law or *"any other significant economic or social disadvantage."* In this view, it is of the essence to note that many public authority liability laws offer only pecuniary reimbursement to injured parties.[129] The important question arises if it is possible to quantify the damage caused by the violation of GDPR. The answer shall be yes. Even in cases where damage is not distinct like if prospective job applicant was denied of job opportunity due to unlawful processing of his data, lost the job or credit card data were leaked and financial loss occurred, there exist models of calculating the value of personal data regardless their (mis)use. As a starting point, the methodology for evaluating personal data from the Organisation for Economic Co-operation and Development (OECD).[130] Methodologies proposed by OECD are based on calculations of (i) financial results for data, (ii) market prices for data, (iii) expenditure of data losses or breaches, (iv) assessment of prices of data in illegal markets, (v) value of data based on surveys and economic experiments or (vi) willingness of data subjects to pay to protect their data.[131] Most of these methodologies are based on market

[129] See § 1 (1) AHG and § 17 Slovak Act on Liability of Public Authorities.

[130] OECD. Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. OECD Digital Economy Papers, No. 220. OECD Publishing, Paris. In: *OECD iLibrary* [online]. 2. 4. 2013 [2020-03-31]. Available at: <http://dx.doi.org/10.1787/5k486qtxldmq-en>.

[131] MALGIERI, G., CUSTERS, B. Pricing Privacy – the right to know the value of your personal data. *Computer Law & Security Review*. 2018, Vol. 34, p. 296.

valuations. This may not fully fit in the case of public authorities as they provide public services without the primary aim of raising revenue. However, it is not excluded to use the market value of specific personal data to calculate damages in case of breach of data protection rules by public authorities as the same data may be involved, only the entity is different. What is more, calculations based on the cost of a data breach shall still be highly relevant for private and public authorities as well.

Other methodologies presented by the doctrine also relate to the market value of personal data e.g. in terms of advertising.[132] Finding the correct methodology for evaluating the value of personal data is not only essential towards calculating damages in case of liability of public authorities, but also from the point of commercial use of public sector information allowed by EU legislation.[133]

4 CONCLUSIONS

Personal scope of GDPR is reserved for specific entities recognized by data protection law – controllers and processors. This binary differentiation is widely criticized but doctrine nevertheless remains applicable and being actively interpreted by CJEU. When it comes to liability, there was a significant shift from Directive 95/46/EC to GDPR. Firstly, some concepts including joint controllers were clarified and attributed liability (although the division is responsibility is still vague). Secondly, processors can be held liable from breach of duties specifically prescribed by GDPR or not compliance with instructions of controllers. The liability regime for the controller remains roughly the same.

In general, public authorities remain in a special position compared to private law entities. This status derives mainly from specific tasks endowed to these entities, financing from national budget and exercise of public authority. However, these specifics are not essential when it comes to the processing of personal data and compliance with GDPR.

One of the open clauses of GDPR allows EU member states to provision fining of public authorities in light of national data protection culture and laws. Three groups of countries emerged being member states prohibiting the fining of public authorities, members states setting up specific rules and conditions for fining public authorities and member states that did not regulate the issue at all and left the possibility for fining public authorities in line with GDPR and national data protection laws. In case, that fines are limited, it is of the essence to examine specific national laws regulating liability for damage of public authorities. By comparing the respective laws of Slovakia and Austria it shall be noted that both laws face obstacles regarding specifics of claiming damages in the data protection area using the legislation offered. Difficulties relating to what exactly amounts to the exercise of public authority and limited scope of these laws.

[132] PETKOVA, B., HACKER, P. Reining in the Big Promise of Big Data: Transparency, Inequality and New Regulatory Frontiers. *Yale Law School: Lecturer and Other Affiliate Scholarship Series*, paper 13.

[133] See Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, pp. 56–83.