THE US LESSONS FOR THE EU PERSONAL DATA BREACH NOTIFICATION: PART II – THE EU REGULATORY PERSPECTIVE AND DISCUSSION OF THE BENEFITS AVAILABLE FROM US EXPERIENCE

František Kasl*

Abstract: *The new obligation to notify personal data breaches under Articles 33 and 34 of the General Data Protection Regulation 2016/679 can be seen as a reflection of the US regulatory approach to security breach incidents, which has an established tradition since the enactment of Security Breach Information Act in California in 2002. The contribution presents in two parts the relevant legal frameworks of the US and the EU, in order to provide a discussion on their similarities and differences. The aim is to identify available intellectual stimuli to the respective academic debate regarding interpretation, application and specification of the EU provisions based on inspiration from the US experience. The Part II adds the insight into the respective EU regulatory approach and contains the discussion of the parallels of the US and EU frameworks and available insight to be drawn from this doctrinal research.*

Keywords: *Personal data breach, security breach, notification obligation, US law, GDPR*

INTRODUCTION AND SUMMARY OF PART I

The first part of this contribution set out the stage for the discussion by describing the multitude of forms that a data breach may take, in particular while considered as cyber security incident, and the increasingly harmful impact it brings to the affected individuals and breached entities in the modern digitalized society. Pursuant to this, we explained the challenges connected with jurisdiction-specific legal definition of this event and established that for this contribution, data breach shall be primarily understood as an unauthorized acquisition of personal data that compromises their confidentiality, integrity or availability, excluding certain good faith acquisitions. This interpretation is more restricted than that applicable to EU legislation, as shall be explained further, however this limitation is necessary in order to be able to set the EU and US framework side by side and discuss possible benefits from perceiving them in this parallel setting.

We do not aim to conduct a cross-jurisdictional comparison of the EU and US data breach notification framework, being fully aware of the numerous more or less significant differences of the respective legal systems, which leaves the methodology for such comparison too challenging to apply to this issue. The most significant features of the US legal system relevant to this issue were highlighted in the previous part and shall be touched upon also in the discussion. However, we attempt to take upon the open call to data protection scholarship by *Lee A. Bygrave*, who asserted that "[n]*onetheless, legal research ought at the very least to ascertain basic similarities and differences between various national and*

* Ing. Mgr. František Kasl is a Ph.D. student at the Institute of Law and Technology, Faculty of Law, Masaryk University in Brno, Brno, Czech Republic

international regulatory frameworks with a view to highlighting possible conflicts, issues and strategies. And it ought, at the very least, to seek to find benchmarks for assessing the relative effectiveness of the respective frameworks."[1] Therefore, the discussion presented in this part is aimed towards looking for transferable experience or insights from the US data breach notification setting that can be beneficial for the doctrinal interpretation and analysis of the rather recent EU legislation with similar scope, aim and conceptual basis.

As was presented in detail in the previous part, the US legislation on data breach notification is a mosaic of similar-but-not-same US-state statutes, which is complemented through sector-specific federal legislation for the financial and medical sector entities. The complexity of the framework is further increased through similarly heterogenous application and enforcement. It was shown that despite US legal tradition strongly linking the interpretation of statutes to judicial precedents, the case law related to data breach, despite being quite numerous, very rarely leads to judgement, but rather ends up with settlement or dismissal on procedural grounds. The reasons for this were elucidated, and other applications of the legal framework were identified, in particular the joint actions by Attorney Generals pursuant to the most damaging data breaches or important activity by the Federal Trade Commission, deriving its authority from broad interpretation of "unfair or deceptive acts or practices".

This second part of the contribution looks on the approach to personal data breach notification in the EU, with obvious focus on the origin and interpretation of Articles 33 and 34 GDPR.[2] The main feature is then the aim of this two-part contribution, i.e. the discussion of the benefits or insights available to EU data protection scholarship from the previously described US setting and experience.

2. PERSONAL DATA BREACH NOTIFICATION IN THE EU

The origin of the personal data breach notification in Europe goes to the adoption of Directive 2009/136/EC,[3] which amended the Directive 2002/58/EC on privacy and electronic communications and introduced the notification obligation to the providers of publicly available electronic communications service in the EU. The definition and concept of the obligation established through this legislation was later fully taken up in GDPR.[4]

There is also other sector-specific or partially overlapping legislation related to notification of data breaches in current EU legislation, the focus is, however, mostly not on the

[1] BYGRAVE, L. *Legal Scholarship on Data Protection: Future Challenges and Directions. Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde Liber Amicorum Yves Poullet. 1*. Brussels: Larcier, 2018, p. 499.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). EUR-Lex.

[3] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009 L 337/11. EUR-Lex.

[4] EUROPEAN COMMISSION. *Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. COM(2012) 11 final 2012/0011 (COD). 2012. p. 7. EUR-Lex.

protection of personal data, but on the integrity of the information system[5] or availability of the provided service.[6] The broadening of scope of notification obligation introduced by GDPR was foreshadowed by intermediary national legislation in the Netherlands in 2016[7] and in Germany in 2017.[8]

Nevertheless, the obligation set by Article 33 and 34 GDPR represents as of now the core of EU approach to smart regulation of personal data breach events as well as necessary transparency towards data subjects in order to mitigate the ensuing risk of harm caused by the subsequent misuse of the acquired personal data.

2.1 Legislative history of the GDPR provisions

The idea of notification obligation encompassing all forms of personal data processing and all kinds of data controllers was actively debated already during the adoption of the above-mentioned amendment to the Directive 2002/58/EC. In 2009 the European Parliament formulated a call for similar instrument applicable without sector limitation, arguing that *"[…] [t]he interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority."*[9] This intention was taken up by the European Commission and the instrument was recast as a generally applicable notification obligation in its opening communication on the Data protection reform from 2010.[10] Support was expressed also by the European Data Protection Supervisor in the corresponding opinion to this EC communication issued in 2011.[11]

2.1.1 Proposal of the European Commission

The wording of the Articles 31 and 32 of the EC proposal (later to become Art. 33 and 34 GDPR) expressly built on the structure of the instrument introduced by Directive 2009/136/EC.[12] The proposed Article 31(33) included strict timeframe of notification to supervisory authority within 24 hours after having become aware of the personal data breach.[13] Communication to affected data subject was according to Article 32(34) due under a low threshold of it being "[…] *likely to adversely affect the protection of the personal*

[5] Art. 14 and 16 of the NIS Directive 2016/1148.
[6] Art. 96 of the PSD2 Directive 2015/2366 or the Art. 19 of the eIDAS Regulation 910/2014.
[7] DE BRUYNE, M. F. Data breach notification and the risk of over-notification under the GDPR. A comparative analysis of US and EU experiences in practice. Master's Thesis. In: *Tilburg University* [online]. 5. 6. 2016 [2020-04-17]. Available at: <http://arno.uvt.nl/show.cgi?fid=140479>. p. 51.
[8] Section 42a Bundesdatenschuztgesetz, BGBL, 2017, Part I No. 2097.
[9] EUROPEAN PARLIAMENT. Position of the European Parliament EP-PE_TC2-COD(2007)0248. In: *European Parliament* [online]. 6. 5. 2009 [2020-04-17]. Available at: <europarl.europa.eu>. p. 21.
[10] EUROPEAN COMMISSION. *Communication from the Commission COM/2010/0609 final.* 4. 11. 2010. EUR-Lex.
[11] HUSTINX, P. Opinion of the European Data Protection Supervisor on the Communication from the Commission In: *European Data Protection Supervisor* [online]. 14. 1. 2011 [2020-04-17]. Available at: <https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf>. p. 17.
[12] EUROPEAN COMMISSION. *Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* COM(2012) 11 final 2012/0011 (COD). 2012, p. 10. EUR-Lex.
[13] Ibid. p. 60.

data or privacy of the data subject […]."Exception from the communication obligation in paragraph 3 related to satisfactory demonstration of appropriate technological protection measures that rendered data unintelligible to those not authorised to access it.

Article 31(33) also included later abandoned paragraph 5 that incorporated specific empowerments for the EC to adopt delegated acts specifying the criteria and requirements for establishing the data breach and for the particular circumstances, in which a controller and a processor is required to notify the personal data breach. Article 32(34) contained similar paragraph 5 concerning specification of criteria and requirements as to the circumstances, in which a personal data breach is likely to adversely affect the personal data. Even this formulation did not remain in the final wording of GDPR.

2.1.2 Text adopted by the European Parliament

The text, adopted by the EP in 2014 by 621 out of 653 votes,[14] introduced noticeable changes to the wording of the discussed articles.[15] The 24 hours deadline in Article 31(33) was abandoned for general formulation of notification without undue delay. New paragraph was introduced, which required the supervisory authority to keep a public register of the types of breaches notified. The conditions for communication to the data subject under Article 32(34) were broadened through adding into consideration aside from privacy also other rights or legitimate interests of the affected individuals. The contents of the communications and its form were reinforced and extended. Competency pursuant to paragraph 5 in both articles was to be transferred to the newly established European Data Protection Board (EDPB), which was tasked with issuing guidelines, recommendations and best practices for the abovementioned aspects as well as for the determination of undue delay. The previously expressed authority of the EC in paragraph 6 to lay down standard format of notification and applicable procedure was abandoned.

2.1.3 Text adopted by the European Council

The Council adopted in 2015 a competing wording of a compromise text modifying the original EC proposal.[16] This version offered third and rather cropped formulation of the relevant provisions. Both communication and notification obligation thresholds were significantly raised by being trigger only "[w]*hen the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage* […]."[17] The maximal permissible timeframe for

[14] The History of the General Data Protection Regulation. In: *European Data Protection Supervisor* [online]. 8. 12. 2016 [2020-04-17]. Available at: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>.

[15] EUROPEAN PARLIAMENT. European Parliament legislative resolution COM(2012)0011 – C7-0025/2012 – 2012/0011(COD). In: *European Parliament* [online]. 12. 3. 2014 [2020-04-17]. Available at: <europarl.europa.eu>.

[16] COUNCIL OF THE EUROPEAN UNION. Interinstitutional File: 2012/0011 (COD). In: *European Council* [online]. 11. 6. 2015 [2020-04-17]. Available at: <data.consilium.europa.eu>.

[17] Ibid. pp. 119–120, Art. 31 para. 1 and 32 para. 1.

notification to the supervisory authority was set to 72 instead of the initial 24 hours after becoming aware of it. Exceptions from the notification as well as communication obligations were expanded or newly added, mainly for encrypted data or effective reactionary measures.[18] The contents of the notice where set on more flexible wording.[19] Paragraphs of Art. 31(33) and 32(34) concerning the issuance of guidelines, specifying acts or standard formats were abandoned, with no substitute proposed in Article 66(70) concerning the tasks of EDPB or elsewhere in the proposed text.[20]

2.1.4 Text proposed by European Data Protection Supervisor

The EDPS subsequently elaborated a comparative table of the above described GDPR texts proposed by EC, EP and the Council respectively and enriched this foundation for ongoing trialogue with a fourth suggested wording prepared by the EDPS.[21] This version considered the core aspects most likely acceptable across the trialogue and presented thereby a rather minimalistic wording of the provisions. Nevertheless, the final text of the GDPR closely resembles this EDPS proposal. It linked the notification obligation with likely risk to the rights and freedoms of individuals and set the required timeframe to 72 hours.[22] A rather vague encouragement of guidelines, in particular for risk assessment, elaborated by EDPB was proposed.[23] These then found their way in Article 70 GDPR describing in one place the tasks of EDPB, specifically para. 1 lit. g, rather than being dispersed through the regulation. On the other hand, the suggested provision on communication to data subjects contained low threshold standard, which was in the final wording of GDPR replaced by higher threshold as proposed by the Council.[24] Similarly, with regard to exceptions from the communication obligation, the EDPS proposal followed the general formulation of the EC proposal, but the final text is based on the extension proposed by the Council.[25]

2.2 Relevant provisions of GDPR

As for the current wording of GDPR that is the result of the trialogue compromise, the core aspects of the personal data breach notification and communication obligations remained largely unchanged from the original EC proposal till the final norm that came

[18] Ibid. pp. 119 and 121, Art. 31 para. 1a and Art. 32 para. 3 lit. a-b.
[19] Ibid. p. 119, Art. 31 para. 3.
[20] Ibid. pp. 120–121, Art. 31 para. 5–6, Art. 32 para. 4-6.
[21] EUROPEAN DATA PROTECTION SUPERVISOR. Opinion 3/2015 (with addendum) Europe's big opportunity. In: *European Data Protection Supervisor* [online]. 9. 10. 2015 [2020-04-17]. Available at: <https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf>; EUROPEAN DATA PROTECTION SUPERVISOR. Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. In: *European Data Protection Supervisor* [online]. 27. 7. 2015 [2020-04-17]. Available at: <https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf> .
[22] EUROPEAN DATA PROTECTION SUPERVISOR. Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendation. In: *European Data Protection Supervisor* [online]. 27. 7. 2015 [2020-04-17]. Available at: <https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf>. p. 169.
[23] Ibid. p. 173.
[24] Ibid. p. 174.
[25] Ibid. pp. 175–177.

into force on 25th May 2018. The definition of personal data breach is directly based on the definition introduced by the Directive 2009/136/EC: *"'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*[26]

The notification obligation in Article 33 GDPR retained the low risk threshold proposed by EDPS and timeframe of 72 hours suggested by the Council. The exceptions proposed by the Council were not passed, but neither was the public register of notified personal data breaches suggested by EP. The communication to the data subject under Article 34 GDPR on the other hand follows the high-risk threshold contained in the Council version and retained significant portion of the exceptions also proposed therein.[27] A notable exception to communication that was proposed by the Council, but not adopted in the GDPR concerns communication, that *"would adversely affect a substantial public interest."*[28]

It can be concluded from this structure that the notification towards supervisory authority should take priority over communication to the data subjects. This approach is strongly contrasting to the one in the US legislation and reflecting the deeper differences in the mechanisms for protection of individual's rights and interests under US and EU law, which have to be taken into consideration.

The risk to the rights or the legitimate interests of affected data subjects giving rise to the notification obligation shall be interpreted in accordance with recital 75 as situations that may result in physical, material or non-material damage, in particular "[…] *discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage.*" In this regard, the broad understanding of personal data under European data protection law, as any information, electronic or not, relating directly or indirectly to an identified or identifiable natural person,[29] needs to be seen as significant enhancer of the scope of personal data breach notification in comparison to the previously described US frameworks under state or federal statutes.

The obligation is applicable to the controller, whereas the processor must notify the controller without undue delay after becoming aware of the personal data breach.[30] It is suitable to note, that the awareness of data breach assumed in the GDPR provisions must be interpreted in connection to the broader personal data security obligations of the controller and processor. This in consequence leads to similar meaning as the one contained in US HITECH Act, which presumes awareness at the moment, when the

[26] Art. 4 no. 12 GDPR.
[27] Art. 34 para. 1 and 3 GDPR.
[28] EUROPEAN DATA PROTECTION SUPERVISOR. Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. In: *European Data Protection Supervisor* [online]. 27. 7. 2015 [2020-04-17]. Available at: <https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf>. p. 177.
[29] Art. 4 no. 1 GDPR.
[30] Art. 33 para. 2 GDPR.

data breach would have been discovered, if reasonable diligence was exercised, even if it was not.[31]

The minimal content of the notification pursuant to Art. 33 para. 3 GDPR fully reflects the changes to the original EC proposal made in the Council version. The notification to the supervisory authority shall contain: a description of the nature and scope of the personal data breach; contact details of the controller (or his Data Protection Officer); likely consequences of the breach; and measures taken or proposed to mitigate the possible adverse effects. The communication to the data subject pursuant to Art. 34 GDPR shall contain similar information in plain and clear language, however, the nature and scope of the personal data breach may be omitted.[32]

Controllers are obliged to document all personal data breaches, even if they do not evaluate them as necessary to notify to the supervisory authority or communicate to the data subjects.[33]

The authority to issue guidelines, recommendations and best practices for establishing personal data breach events and determining preconditions and timeframe for notification falls to the European Data Protection Board (EDPB) pursuant to the Art. 70 para. 1 lit g GDPR. Initial interpretative guidelines were issued by Article 29 Data Protection Working Party (predecessor body to EDPB under Directive 95/46/EC) in October 2017.[34] Applicable as general guidance remain also recommendations on assessment of severity of personal data breaches by ENISA from 2013.[35] These documents form the basis for the much-needed specifications for effective implementation of the new general notification obligation by all forms and sizes of controllers and processors, nevertheless, the broad scope of these documents precludes necessary detail of guidance for individual sectors, business models or specific scenarios. GDPR foresees such guidance primarily from the codes of conduct elaborated by bodies representing various categories of controllers and processors pursuant to Art. 40 GDPR. Nevertheless, activity in this regard, in particular with respect to personal data breach notification guidance remains even now rather scarce, forcing most controllers to derive applicable interpretation of the obligation from the abstract wording of the provisions and general recommendations provided by Article 29 Data Protection Working Party and ENISA documents.

The available data for the past two years of this obligation indicate a wide spread of notified incidents throughout the EU. The low threshold and ambiguous interpretation of the obligation are likely to lead controllers to overreporting on identified personal data breaches,[36] however the differences among Member States are unlikely due to differences

[31] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679 18/EN WP250rev.01. In: *European Commission* [online]. 6. 2. 2018 [2020-04-17]. Available at: <https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827>. p. 11.

[32] Art. 34 para. 2 GDPR.

[33] Art. 33 para. 5 GDPR.

[34] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Personal data breach notification under Regulation 2016/679 18/EN WP250rev.01*.

[35] ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. In: *ENISA* [online]. 20. 12. 2013 [2020-04-17]. Available at: <https://www.enisa.europa.eu/publications/dbn-severity>.

[36] BURTON, C. Article 33. In: C. Kuner et al. (eds.). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, New York: Oxford University Press, 2020, p. 646.

in threat level or number of controllers, but rather a sign of varied personal data protection tradition and uneven position of the supervisory authorities in different Member States. To provide a specific example, the number of notified personal data breaches in Netherlands, which had notification obligation implemented on national level already before GDPR came into force, was over the period between 25th May 2018 and 27th January 2019 at 15 400 and over period between 28th January 2019 and 27th January 2020 another 25 247 reported incidents. In comparison, countries like the Czech Republic, Hungary or Romania received in these two periods merely low hundreds of notifications, despite being of similar size.[37]

GDPR provided the supervisory authorities with unified toolbox of powers, which include investigative powers pursuant to Art. 58 para. 1 GDPR as well as effective corrective powers enlisted in para. 2. These include in particular powers to order the controller to bring processing operations into compliance in a specified manner and within a specified period; to order the controller to communicate a personal data breach to the data subject; to impose a temporary or definitive limitation including a ban on processing; and to impose an administrative fine pursuant to Article 83 reaching up to 10 000 000 EUR (or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher). We can already see first cases, where national supervisory authorities imposed administrative fine for breach of the notification obligation. The largest fine so far in the amount of 600 000 EUR received Uber in late 2018 for a year delayed notification of large personal data breach. To be specific, however, this fine was imposed based on the Dutch national transitory legislation preceding the coming into force of GDPR.[38] Administrative fines for delayed or omitted personal data breach notification pursuant to GDPR provision were issued in Lithuania (amount equivalent to 61 500 EUR), Hungary (amount equivalent to 34 375 EUR), Germany (20 000 EUR) or Romania (amount equivalent to 20 000 EUR).[39] This shows the above described framework as established, yet there still remain significant obstacles to proper utilisation of the notifications in order to achieve intended benefits connected with this aspect of smart regulation and transparency towards data subjects.

3. DISCUSSION

The initial sections of the Part 1 of this contribution identified the prevalence and impact of personal data breaches concerning electronic records. It highlighted the inconspicuous ubiquity of cyber security incidents that lead to unauthorized disclosure and processing of personal data by third parties, mostly for financial gain and often with serious consequences for the virtual identity of the individual data subjects. There were also

[37] DLA PIPER'S CYBERSECURITY AND DATA PROTECTION TEAM. DLA Piper GDPR data breach survey: January 2020. In: *DLA Piper* [online]. 2020 [2020-04-17]. Available at: <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>. p. 6.

[38] AUTORITEIT PERSOONSGEGEVENS. Dutch DPA: fine for data breach Uber. In: *Autoriteit persoonsgegevens* [online]. 27. 11. 2018 [2020-04-17]. Available at: <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber>.

[39] CMS. Fines Database. In: *GDPR Enforcement Tracker* [online]. 2020 [2020-04-17]. Available at: <http://www.enforcementtracker.com>.

provided references to security landscape reports and threat analyses pointing out that the trend is strongly and steadily towards increasing number, impact and sophistication of these incidents, leading to more detrimental impact on increasing number of data subjects every year. Additionally, new technologies, like the internet of things devices, and gradual transition of the business and social interactions towards predominantly virtual communication, further hastened by the quarantine measures of the covid-19 pandemic, add further to the significance of this issue.

The notification obligation as established in the US law and later adopted in EU law, leading to the general obligation Art. 33 and 34 GDPR, presents a robust regulatory concept for mitigation of the impact connected with these detrimental events. Response to cyber security incidents affecting personal data needs to be coordinated in order to be effective, given the nature of information and speed of its dissemination in the cyberspace. Therefore it needs to include not just the affected controller or processor, but also supervisory authority, allowing for broader view of the overall landscape development, and further the individual data subject, who is in best position to mitigate the impact by adjusting his or her virtual identity settings or pursuing actively measures to curtain the threat related with the leaked personal data. Such open communication, transparency and coordination are key to effective response, however, the US as well as EU experience show numerous challenges limiting the functional implementation of this concept in everyday business setting.

3.1 Main challenges to functioning of the personal data breach notification

In our opinion, there are three main challenges to functioning of the personal data protection notification. First is the setting of adequate motivation for compliance, either by trade-off or by enforcement. The obligation to notify on cyber security incidents is in principle conflicting with the interests of the notifying entity, in particular given specific obligations regarding adequate personal data protection and potential opening of the entity to administrative fines for non-compliance with these requirements. Even if the main benefit of the notification obligation is mitigation of the information asymmetry by the primary victims, i.e. affected data subjects, or the regulator, the rationale for the notifying entity is primarily based on impact on its interests. Relatively low imposed sanctions, limited probability of their enforcement and high complexity of associated procedures contribute to less motivation towards compliance. Making compliance with notification obligation more attractive alternative than non-compliance (in economical sense of weighing probable benefits and costs) is crucial for making is a functional transparency instrument.[40]

Next to the motivation towards compliance stands sufficient clarity of the obligation and its boundaries. The scope of personal data protection law is, in particular in the EU law, very broad, encompassing the full plethora of business models, activities and pro-

[40] GARCIA, M. E. The Economics of Data Breach: Asymmetric Information and Policy Interventions Dissertation thesis. In: *The Ohio State University* [online]. 2013 [2020-04-17]. Available at: <https://etd.ohiolink.edu/ap/10?0::NO:10:P10_ACCESSION_NUM:osu1365784884>. pp. 180–181.

cesses. Translation of legal obligations into specific applications and measures, in particular of technical nature, is a continuous challenge. Guidelines, best practices and codes of conduct are therefore great enablers of compliance, whereas their lack or ambiguity may prevent adequate compliance even in case of sufficiently motivated entities.

With challenges posed by the limited motivation of the obliged entities towards compliance and lack of clarity of the obligation that hinders implementation into practice, the focus of the entities should be targeted on issues posing the highest risk, where proper compliance provides for maximum mitigating impact. Despite the broad scope of personal data processing activities, the related risks for data subjects differ greatly. Digitally stored and processed data differ from paper-based databases. Protective impact of encryption varies. Certain sectors or business models predetermine increased likelihood of high impact incidents. Protection of some datasets is aligned with the core interests of the entity, whereas other may be perceived secondary, despite their sensitivity or potential impact on the data subjects. The entities may be aware of these differences; however, their interests are not likely to be aligned in all cases with those of the data subjects. The priorities in this regard need therefore to be identified by the regulatory framework and promoted by the regulators.[41]

3.2 Comparison of US and EU approach

Each set of legal provisions presented in this contribution provided a unique mix of measures and conditions aimed at tackling these three challenges. Narrow scope of core terms like "security breach" or "personally identifiable information" in the US law, as well as multiple exceptions or thresholds reflect focus on notification in case of major personal data breaches. Limitation to digitally process personal data or enumerated forms of personal data provides further clarity and lower threshold for compliance. Sectoral legislation similarly sets more specific priorities and adjusts the requirements to conditions and challenges typical for the business models and processing activities.

At the same time, however, the US situation indicates limits that follow from a lack of unified basis of the regulatory structure. The fragmentation in terminology and minor variations in the parameters of the instrument across the US statutes creates additional burden for entities pursuing compliance. The common basis created by Articles 33 and 34 GDPR should allow for better functioning structure than in the US without a federal law. The challenge for EU personal data breach notification then at this point stems mainly from lack of clarity of the obligation in the 0case-by-case setting. As explained in the earlier section of this part, the current wording of the articles represents largely a base compromise that needs additional specifications and interpretations to be adequately implemented. The general rule is set and the terms are defined. Now is needed the fine-tuning through exception, best practices, sectoral guidelines or priority areas.

[41] SKROUPA, CH. GDPR Priorities: Public Companies Must Urgently Handle Data Breaches. In: *Forbes* [online]. 20. 7. 2018 [2020-04-17]. Available at: <https://www.forbes.com/sites/christopherskroupa/2018/07/20/gdpr-priorities-public-companies-must-urgently-handle-data-breaches>.

The EU personal data protection framework is built towards the goal of high level of protection for all data subjects in all situations. Nevertheless, the road towards making this a functional reality goes through gradual improvement. Similarly, the mitigation of information asymmetry with regards to personal data breaches should rest on gradual progress, first concentrating the focus of the entities and authorities on the areas with highest risk of major data breaches and greatest subsequent detrimental impact. This regulatory strategy is inherent in the current personal data framework; however, the priorities and gradation are not expressly set and clearly communicated. As such, there remains a significant uncertainty about the proper approach to compliance.

3.3 Possible lessons from the US experience

To search for this approach, we consider as valuable input to observe the practical implementation of the framework in the US, as inspiration for aspects that seem to work as well as those, which seem to fail.

As follows from both parts of this contribution, the landscapes of personal data breach notification in the US as well as the EU settings are rather complex and involve multiple facets that need to be carefully considered in case of any attempt for transposition of experience between these legal systems. Despite overall similarity of the US and EU legal systems, there are numerous minor systematic and conceptual differences underlaying and permeating the legal regimes of personal data protection in both jurisdictions. These then pose barrier between the equation of the approaches to particular issues. The main differences coming into play here were described in detail in the Part 1 of this contribution and it is with these limits in mind that we formulate the following considerations.

The US legislative experience with data breach notification indicates benefits of clarity and focus of this instrument as well as challenges connected with its fragmentation and ambiguity. The multitude of approaches and similar-but-not-the-same terminology present major obstacles to functional compliance and enforcement in the US. The unified EU legislative framework in the form of GDPR on the other hand provides crucial step that was so far not achieved in the US setting. However, further coordination and cooperation in this area is necessary, in particular in order to be able to effectively respond to the major personal data breaches that affect entities active in multiple EU Member States[42] or to cascading incidents spreading indiscriminately throughout the global network.[43] Core projects in this regard are the Pan-European Personal Data Breaches Exercises organized by the Joint Research Centre together with the Directorate-General for Justice and Consumers of the European Commission and Data Protection Authorities of EU Member States.[44]

[42] RODRIGUEZ, S. Facebook hack affected 3 million in Europe, creating the first big test for privacy regulation there. In: *CNBC* [online].16. 10. 2018 [2020-04-17]. Available at: <https://www.cnbc.com/2018/10/16/facebook-hack-affected-3-million-in-europe-first-big-test-for-gdpr.html>.

[43] ZIMBA, A., CHISHIMBA, M. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. *European Journal for Security Research*. 2019, Vol. 4, No. 1, pp. 3 et seq.

[44] MALATRAS, A. et al. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review*. 2017, Vol. 33, No. 4, pp. 458 et seq.

On the other hand, the EU-adopted broad approach to personal data breach notification, encompassing diverse spectrum of entities and situations without clear differentiation or prioritization, hinders efficient compliance for many entities. The rather narrow scope of US data breach notification obligations supports focus on major threat factors and critical situations. This allows for clearer guidance and greater resulting effect on data breach impact mitigation. The specificity of the tools may be increased on several levels, either in the text of the legislation or through explanatory guidelines. The basic level is the concept of scope and focus on certain areas of personal data processing or certain forms of personal data breach. The situation in the financial sector, medical sector, e-commerce sector or social media provides to a large degree distinct challenges and threat scenarios from other fields that utilize lower volumes of sensitive personal data in the core business activities. Digitalisation and new technological trends further make threats related to certain distinct areas overshadow the standard threat scenarios and require more specific approach. Example of such trend is the gradual emergence of ubiquitous processing through the internet of things devices.[45]

The thresholds for communication or notification of personal data breach are set in ambiguous legal terms that require comprehensible translation into criteria and values than can be incorporated into business models and technical calculations. The efforts of the controllers should be mobilized to deal primarily with the major threats, utilizing the interconnection of the personal data breach notification obligation with other obligations under cyber security regulation or ICT security standards. The existing guidelines and rules by US authorities supervising data breach notification in various areas should serve in this respect to a large degree as sample experience that can be built upon and refined for EU setting.

Additionally, several components of the US law may be considered for adoption in the EU data protection framework. Firstly, the exceptions from the notification or communication obligation or its strict timeframe should be clearly and transparently set. This should take into consideration the various situations, when disclosure of the information may be detrimental to law enforcement efforts; when restoration of the system integrity or investigation of the event should take priority; or when sector specific situations constitute data breach under the general definition, but lack the related detrimental effect. Under consideration should further come publicly accessible registries of personal data breaches, similar to the one operated by HHS,[46] which may contribute to increased transparency and modify the incentives of obliged entities for greater compliance. Proposal for such registry was present in the European Parliament version of GDPR.[47]

An aspect worth mentioning that was omitted in the previous sections is the role of whistle-blower tradition in the US, including their established protection and recognition

[45] SCHNEIER, B. *Click here to kill everybody*. New York: W.W. Norton & Company, 2018.

[46] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. In: *U.S. Department of Health and Human Services* [online]. 2020 [2020-04-17]. Available at: <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>.

[47] EUROPEAN PARLIAMENT. European Parliament legislative resolution COM(2012)0011 – C7-0025/2012 – 2012/0011(COD). In: *European Parliament* [online]. 12. 3. 2014 [2020-04-17]. Available at: <europarl.europa.eu>. p. 178.

with regard to cyber security issues like occurrence of personal data breaches pursuant to *inter alia* Sarbanes-Oxley Act of 2002.[48] The recent progress made in the EU in this area through adoption of the harmonised directive is likely to soon have major impact on the disclosure of personal data breaches,[49] which already sees increased post-GDPR activity.[50]

The last aspect of the US data breach notification structure that is to be discussed in this contribution is the role of private litigation in the structure of compliance enforcement. The US experience indicates that private litigation in issues concerning personal data breaches, despite the well-established tradition of class actions, including enhancing tools like the concept of punitive damages, faces major obstacles. The existing evidence of private class actions based on diverse causes of action ranging from breach of contract, breach of duty or misrepresentation through breach of good faith or breach of warranty to specific grounds for statutory damages following from federal as well as state-level statutes shows versatility of data breach situations and difficulty of tackling this phenomenon within the established civil law framework.[51] The high share of dismissals on record may largely be the consequence of US-specifics,[52] in particular the fragmented nature of the legislation combined with established procedural requirements set forth by the federal courts, but the challenges related to identification of scope, assessment of harm and attribution of compensation are likely to be similar in EU setting as well. Under these circumstances is understandable the predominance of settlement agreements in data breach cases and incorporation of the related costs under the standard costs of doing business rather than functioning as compelling incentive.

The EU framework largely avoids this pitfall through preference of sanctions enforced through supervisory authorities. Nevertheless, the efficiency of this approach is dependent on their personnel and budgetary capacities, which are in some Member States disproportionately limited. Combined approach through private as well as public coercion towards compliance may be beneficial in this respect. The tradition of collective redress through class action is present, but not deeply developed, in the European setting.[53] However, progress is being made towards EU collective redress mechanism, which should be utilized also with regard to personal data protection issues.[54] The further encouragement

[48] SWANSON, K., KIRSCH II, T., DUNIGAN, R. Data Breaches in a Whistleblower's World: What You Should Know, Why You Should Know It. In: *ABA Criminal Justice Section Newsletter* [online]. 2013 [2020-04-17] p. 7. Available at: <https://www.crai.com/sites/default/files/publications/Data-Breaches-in-a-Whistleblowers-World.pdf>.

[49] EUROPEAN COUNCIL. Better protection of whistle-blowers: new EU-wide rules to kick in in 2021. In: *European Council* [online]. 7.10.2019 [2020-04-17]. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/>.

[50] RAM, A. Reports from whistleblowers on data breaches almost triple. In: *Financial Times* [online]. 16. 12. 2018 [2020-04-17]. Available at: <https://www.ft.com/content/2bec495a-014e-11e9-9d01-cd4d49afbbe3>.

[51] ROMANOSKY, S., HOFFMAN, D., ACQUISTI, A. Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*. 2014, Vol. 11, No. 1, p. 25 figure 7.

[52] Ibid., p. 19.

[53] EUROPEAN COMMISSION. Report from the Commission on the implementation of the Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union law (2013/396/EU) COM/2018/040 final. 25. 1. 2018. EUR-Lex.

[54] EUROPEAN PARLIAMENT. First EU collective redress mechanism to protect consumers. In: *European Parliament* [online]. 6. 12. 2018 [2020-04-17]. Available at: <http://www.europarl.europa.eu/news/en/press-room/20181205IPR21088/first-eu-collective-redress-mechanism-to-protect-consumers>.

of these possibilities and awareness of some of the potential pitfalls that occurred in the US setup should result in better functional and beneficial framework of personal data breach notification in the EU context.

4. CONCLUSION

This contribution in both its parts focused on the personal data breach notification framework from the US and EU perspective. The aim was to identify available intellectual stimuli to the respective academic debate regarding interpretation, application and specification of the EU provisions based on inspiration from the US experience.

The first part introduced the reader to the issue of personal data breach, in particular concerning electronic records and thereby taking on a form of a cyber security incident. The scope and impact of these incidents were highlighted, as well as continuous trend towards more frequent and disruptive data breaches each year. Following this, the legal definition of personal data breach was presented, leading to identification of the main differences between the US and EU perspective and subsequent limitations applicable to any direct transfer of experience. The major focus of the Part 1 then was to describe the US framework of personal data breach notification.

This part then followed with details on the development and structure of the EU framework for notification of personal data breaches, allowing for a subsequent discussion of challenges related with this concept. Three main challenges were formulated: (i) lacking motivation to exercise compliance; (ii) confusion due to ambiguity of the obligations; and (iii) unclear focus of the obligations diverging the efforts from threats with highest impact. In light of these common challenges, the US and EU approach were discussed and insights were drawn from this parallel view for functional approach to personal data breach notification framework in the EU. The main outcomes of this discussion include a continuous appeal towards clear interpretation of the harmonized rules; coordinated response to major data breaches; differentiation of the obligation for high-risk sectors and specific settings; clearly set focus on the major incidents through implementation of quantifiable thresholds that can be incorporated in the business models and technical calculations; transparently enlisted exceptions from the obligation due to e.g. criminal investigation; set up of a publicly accessible registry of notified personal data breaches; well-structured support for whistle-blowers; and concentrated focus on corrective activities of the supervisory authorities rather than private litigation.