

The 10th International Conference on Ambient Systems, Networks and Technologies (ANT)
April 29 – May 2, 2019, Leuven, Belgium

GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones

Peter Štarchoň^a, Tomáš Pikulík^{a*}

^a Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 820 05 Bratislava 25, Slovakia

Abstract

The core concept of European reform of the law on the protection of personal data, implemented in EU General Data Protection Regulation (GDPR) – European Parliament and Council Regulation No 2016/679 becoming enforceable on 25th May 2018. GDPR as a new framework for unit 500 million of customers has strengthen and unite the aspect of data privacy that retaining the main principles of previous Data Protection Directive 95/46/EC. Regulation brings by its hidden traps, many important new obligations in coherence with tougher regime of data privacy in terms of usage of fines and sanctions for the unwary ones. Thus, in this paper, we refer to data protection principles by the example of mobile operators that affect our everyday lives with reference to assigned problem of collect, process and manage a relatively large amount of our personal data. Analytical and conceptual view of processing customer's metadata and considering right of subject to data portability also reveals and encourage methods for implementing pseudonymization techniques to process them on behind to secure customer's privacy.

© 2019 The Authors. Published by Elsevier B.V.

This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Peer-review under responsibility of the Conference Program Chairs.

Keywords: GDPR ; data privacy ; pseudonymization ; additional data ; non-attributes ; user ; data subject ; controller ; processor ; pseudonymous data ; pseudonymization techniques ; right to data portability ; statistical counting ; phone number transfer ; ePrivacy ; data minimisation

* Corresponding author. Tel.: +421-918-713-838.

E-mail address: tomas.pikulik@fm.uniba.sk

1. Introduction

GDPR promotes trust for us as subjects and EU citizens as well [1] – in terms of credibility, reputation and public standing of responsible provider, certainly and brings new point of view for data protection in terms of coverage of could be possibly strengthen the trust for personal data of concerned subjects through pseudonymization techniques that is revealed by various IT providers that involve them in their tools, services and solutions for data administration and processing. Aim objective of this paper is to identify particular security measures of pseudonymization as a data protection tool that secure consumer privacy described on impact of customer personal data by mobile phone operators in Slovakia.

Paper in introduction part reveals in details basic principles of data protection that are crucial part of GDPR No 2016/679. All interested subjects even though that are controller, processor or data subject have not only rights but also obligations to prevent misuse of personal data. Business models represents the architectural implementation of a strategy [2, 23, 24] and in way of processing personal data these models need to understand its new obligations and paper clarify in detail pseudonymization techniques that enable to protect personal data in safe. GDPR and its principles lies and focus on personally identifying information. On the other hand, it set also new principles of PDP.

To capture the changes defined in Regulation and Directive in Slovak Republic was adopted a New Personal Data Protection Act (Slovak Act No. 18/2018 Coll. on the protection of personal data). In conclusion part we have looked in deep in direct transmission of personal data by Slovak Mobile operators while processing metadata – during direct transmission of personal data of users (existing customers in case of phone numbers transfer to another operator). To sum up the topic for process interconnected with possible data portability - we used primary research methods interviews and surveys. We have summarized actual propositions of Slovak operators and revealed benefits for users that brings innovative services for society with the appropriate personal data protection (PDP).

Nomenclature	
3G, 4G, LTE	Mobile data networks
EAA	European Economic Area
EC	European Council
EDPB	European Data Protection Board
ETNO	Europe's telecommunication network operators
EU	European Union
GDPR	General Data Protection Regulation
G	Giga - unit prefix in the metric system denoting a factor of a billion (10^9 or 1 000 000 000)
IP	Internet Protocol
M	Mega - unit prefix in the metric system denoting a factor of a million (10^6 or 1 000 000)
PAN	Primary Account Number
PbD	Privacy by Design
PDP	Personal Data Protection
PETs	Privacy-Enhancing Technologies
TV	Television

2. Role of Data controller and Processor encourage usage of pseudonymous data of customer

The core concept of European reform of the law on the PDP, implemented in GDPR and its principles lies and focus on personally identifying information and data privacy. GDPR define the role of data controller, data processor and data subject. In short, the data controller will be the one to dictate how and why data is going to be used by the organization – represents the entity that determines the purposes and means of processing of personal data. A data processor simply processes any data that the data controller gives them on behalf of data controller. The data processor does not own the data that they process nor do they control it. Data processor will not be able to change the purpose and the means in which the data is used. Furthermore, data processors are bound by the instructions given by data controller. In GDPR and other privacy laws, the data controller has the most responsibility when it comes to protecting the privacy and rights of the data's subject [3]. On the other hand, GDPR set also new

principles of PDP. Data subject is any natural person, whose personal data are regarded to. For clarification Personal Data is name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identity of that person. If we are focusing on online identifiers, IP addresses, cookies, mobile IPs and even search engines will fall into a scope of GDPR [4]. Only individual natural person may be considered as data subject regardless of his citizenship. In no way may legal person be considered as natural person. Same applies with natural persons – entrepreneurs while acting within their business activity [5]. The core rules seem well-known and familiar for experienced data specialist (e.g. experienced data practitioners before defining position of Data Privacy Officer by Article 20 in specified cases not only for controller but for processor). GDPR brings by its hidden traps, there are also many important new obligations in coherence with tougher regime of data privacy in terms of usage of fines and sanctions for the unwary ones. Aim is to strengthen privacy policy of all interested: data subjects (with its new rights combined with principles of PDP), controllers, processors (in terms of principles). GDPR reveals 7 data protection principles (see Fig. 1) that are listed in Article 5 and both entities - the data controller and data processor must ensure that it complies with all of them.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Fig. 1. Data protection principles according GDPR [6,7,18].

Looking to dive deeper into the GDPR regarding pseudonymizations we can focus as is written in Recital 28 on the explicit introduction of pseudonymization in this Regulation is not intended to preclude any other measures of data protection like existing and well-known encryption. By its ambition to set as a leadership to greater degree of PDP harmonization across EU nations GDPR brings pseudonymized data as a subset of personal data (see Fig. 2b).

Strength and credibility of pseudonymized data is determined by process of two-way of encryption mentioned above – personal data cannot be added to identified person without additional information or a key. Based on GDPR personal data should be pseudonymized in a way that it can no longer be attributed to a single data subject (user) without the use of additional data (see Fig. 2a). This additional data should be kept separate from the pseudonymized data and subject to technical and organizational measures to make it hard to link a piece of data to someone's identity (non-attribution).

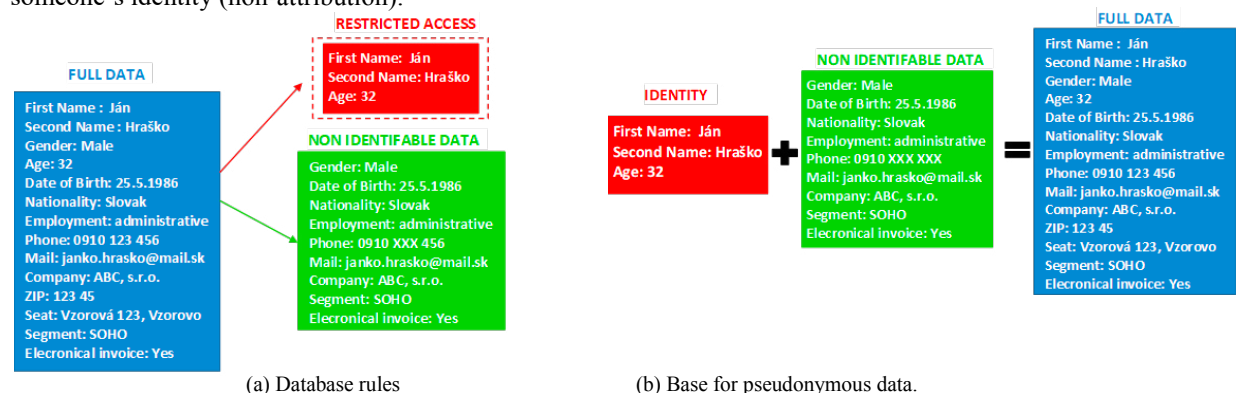


Fig. 2. Pseudonymous data still allows for some form of re-identification (even indirect and remote) [8].

3. Pseudonymization techniques as one of method that fulfills principles of data privacy

Pseudonymization is a security technique for replacing sensitive data with realistic fictional data that [9]:

- Cannot be attributed to a specific individual without additional information which, according to GDPR Article 4 (5), is to be “kept separately and subject to technical and organization measures to ensure non-attribution to an identified or identifiable person.”
- Maintains referential integrity and statistical accuracy, thereby enabling business processes, development and testing systems, training programs, and analysis to operate normally.
- Pseudonymization can be used when realistic data is needed for application development and testing environments, data warehousing, analytical data stores, training programs, or other business processes. It can also be used when exporting data to non-EU/EEA countries.

Pseudonymization can be used when realistic data is needed for application development and testing environments, data warehousing, analytical data stores, training programs, or other business processes. It can also be used when exporting data to non-EU/EEA countries.

Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified [10].

Pseudonymization techniques differ from anonymization techniques. With anonymization, the data is scrubbed for any information that may serve as an identifier of a data subject. Pseudonymization does not remove all identifying information from the data but merely reduces the linkability of a dataset with the original identity of an individual (e.g., via an encryption scheme).

Both pseudonymization and anonymization are encouraged in the GDPR and enable its constraints to be met. These techniques should, therefore, be generalized and recurring. Those in possession of personal data should implement one or other of these techniques to minimize risk, and automation can reduce the cost of compliance. We can differ the pseudonymization techniques that are also actual in case of mobile operators [8] :

- **Scrambling** - techniques involve a mixing or obfuscation of letters. The process can sometimes be reversible. For example, "Janko Hraško" could be scrambled for: "Jknao rHaško"
- **Encryption** - it exhibits the original data incomprehensible and the process cannot be reversed without access to the correct decryption key. The GDPR requires for the additional data (such as the decryption key) to be kept separately from the pseudonymized data.
- **Directory replacement** - method involves modifying the name of subject integrated within the data, while maintaining consistency between values, such as “postcode + city“. For example, replace “Janko Hraško“ by “Elena Tichá“ and maintain “123 45 Vzorovo“.
- **Masking** - technique allows an important/unique part of the data to be hidden with random characters or other data. For example: “0910 123 456” phone mobile number can be stored as “0910 XXX 456”. The advantage of masking is the ability to identify data without manipulating actual identities.
- **Tokenization** - is a non-mathematical approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens. Tokens have no extrinsic or exploitable meaning or value. Tokenization does not alter the type or length of data, which means it can be processed by legacy systems such as databases that may be sensitive to data length and type. That is achieved by keeping specific data fully or partially visible for processing and analytics while sensitive information is kept hidden. For example, tokenization is key for mobile payment security - tokenization protects payment credentials by replacing them with a randomly generated number that resembles the customer’s primary account number (PAN). Only bank and payment processor may read back the PAN not the retailer, so it is another security element in mobile payment process.
- **Data blurring** - uses an approximation of data values to render their meaning obsolete and/or make it impossible to identify individuals. A good example is a typical blurred face in an image (e.g. Google Maps Street views) but in terms of Data Security terms also Age and Date of Birth is possible to Blur with special type of Blur Functions. Date blurring functions follows a format similar to age blurring but use also date as a its input and output (see Tab. 1). Random blur functions are in days and will change month and year if the new date is past the last day of the month or before the first. The blur date function and its possible forms are [11]:

(1)

```

blur_date (DATE, MIN_DATE, MAX_DATE, BLUR_FACTOR)
blur_date (DATE, MIN_DATE, MAX_DATE, BLUR_FACTOR, MODE_DATE, MODE_BLUR_FACTOR)
Example:
Function Calls
/FIELD=(EXPRESSION_AGE=blur_age(AGE, 10), TYPE=NUMERIC, PRECISION=0, POSITION=1,
PRECISION=0, SEPARATOR="|")
/FIELD=(EXPRESSION_DATE=blur_date (DATE, "1986-05-25", 30), TYPE=ISO_DATE

```

Table 1. Example of input and output of this pseudonymization method

Input	Output
34 1986-05-25	44 1986-06-24

3.1. Right of portability and data transmission

Article 20 of GDPR that gives attention to right to data portability also state that data subject has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. Although the GDPR tend to give the right to data subject to transfer its data free of charge, on the other hand the consumer (as a data subject) would finally benefit from its data transmit. As noted above rights to portability as a free of charge right is undoubtedly mentioned in Article 12 (5) whereas in this part common as "Transparent information, communication and modalities for the exercise of the rights of the data subject" directly claim: "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge." Without any question all actions taken by Article 20 is part of it. There is also indisputable role for controller up to data subject where in Article 12 (5) define that any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Since activating GDPR into practice there is outright challenge for controller in area of application settled by Recital 68 whereas stated for personal data of data subject following: "To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller." According this data controllers should be encouraged to develop interoperable formats that enable data portability.

That right should apply where the data subject provided the personal data on the basis of his or her consent [20] or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. Many of companies that operates and run their business in EU have already adopted privacy processes or privacy policy before GDPR entered to a force on 25th May 2018.

3.2. Local specification in Data Privacy

In Slovakia also, the Act that was published in the Collection of Laws under the number 18/2018 Coll on 30th January 2018 as new act on the PDP. New PDP Act that had replaced the Slovak Act No. 122/2013 Coll. on the PDP [11]. Directive and Regulation came into operation at the same day - on 25th May 2018. The New Personal Data Protection Act largely duplicates the provisions of the GDPR, which as a regulation is directly applicable in the Slovak Republic, but also transposes into the Slovak legal order, the so-called "Police" Directive (European Parliament and Council Regulation (EU) No 2016/680) and also uses the option contained in the GDPR, to define categories of exceptions and derogations from the GDPR in the legal systems EU Member States. In terms of Data privacy there is appropriate to mention the role of Constitution of the Slovak Republic, Article 19 (2, 3) [4]:

- Paragraph 2: "Everyone has the right to protection against unwarranted interference in his private and family life."
- Paragraph 3: "Everyone shall have the right to be protected against unauthorized collection, disclosure or any other misuse of his or her personal data."

PDP, especially privacy of their processing, is a sensitive area of fundamental rights and freedoms of natural persons guaranteed by the Constitution of the Slovak Republic. Actual legislation framework set the rules and adoption of principles covered by GDPR strengthen the rights of the concerned person to protect personal data against misuse and unauthorized access. Personal data is a gateway to a privacy of everyone. EU and its representative body as well as local lawgiver and local control body realize the power of unlimited possibilities of communication as a time period of great expansion of IT that actually brought not only benefits but also threats.

Also, both authors Clearwater and Theilová [13] outlined at first step of Data Privacy not to look out only for domestic legislation but also on European Data Protection Board (EDPB) guidelines: The GDPR is still very young legislation; a lot of its clauses are still open to interpretation. We can therefore expect the newly established EDPB to gradually fill in the blanks and clarify certain issues regarding the interpretation of the GDPR, as well as provide guidance and harmonization of enforcement among EU Member States. This attitude for PDP is in line with author Suchánková [14] as a lawyer at an alliance PIERSTONE (network) of lawyers with branches in London, Brussel and Moscow as one of the biggest specialized law teams oriented on the right of technologies, medias and communications of advantages of pseudonymous data:

- Data may be processed beyond the originally defined purpose
- Moderate regulation: exceptions to notification, others responsibilities
- Pseudonymization meets the requirements of Privacy by design (PbD)
- Pseudonymization is security measure

4. Customer's benefits of innovative services - transfer of mobile phone number covered by pseudonymization

As declared by enterprise ETNO they exactly want to hold the line with an approach in line with Article 6 (4) of GDPR balances the benefits of innovative services for society with the appropriate PDP for consumers.

By the definition (TOGAF 2002) the “enterprise” is any collection of organizations that has a common set of goals and /or a single bottom line [15, 23, 24]. To site from ETNO statement for call on Minister for preparing ePrivacy Regulation from 30th of May directly [16]: “As we approach the 8 June Telecommunications Council meeting, we urge Ministers to give a clear signal that rules should allow innovative use of metadata where it is appropriate and justified. To achieve this, we suggest to incorporate the GDPR’s risk-based approach, which makes the Regulation future-proof, by allowing further processing of metadata without consent for purposes compatible with the initial purpose for which the data were collected, subject to compulsory safeguards such as pseudonymization.[†] Such an approach in line with Article 6 (4) of GDPR balances the benefits of innovative services for society with the appropriate PDP for consumers. More work is needed in this regard, since the currently proposed solutions around statistical counting are likely to be interpreted too restrictively and would not allow for data analytics to take place in a variety of accountable business models.”

The statement greeted that GDPR making effect as a new high standard for all players in the digital economy. Cable Europe, GSMA and ETNO’s members have made implementation of the GDPR their highest priority, since the PDP is at the core of their industry’s business model. In this way PDP for customers should be considered as an enterprise model because it represents structure, activities, processes, information, resources, people, behavior, goals, and constraints of a business, government, or other enterprises.

On the other hand, telecom operators are currently still subject to national rules implementing the ePrivacy Directive, which restrict the way they can handle data generated and carried over their networks. In case of controller as mobile operator where direct transmission of personal data from one operator to another operator the consumer would:

- Benefit from mobile phone number transfer financially
- Retrieve and activate new services as a new customer
- Gain advantages connected to group or community of existing customers

[†] More specifically, we suggest including the principle of “further compatible processing” of Article (6) Par. 4 GDPR as a mechanism for processing metadata in Article (6) Par. 2 of the proposed ePrivacy Regulation.

4.1. Footnotes Local overview of benefits of data transmission - Slovak mobile operators

We have mapped this situation and protentional benefit for transmission of personal data of innovative services for society with the appropriate PDP in case of Slovak mobile operators – concretely during service of phone number transfer. It is still relevant fact on our local market because more than 200 000 people transfer their mobile phone number to another mobile operator every year (direct statistics would be made public in the beginning of the 2019). Slovakia has a specific situation where market is divided for big three - Orange, Telekom, O2 and challenged by national Slovak Operator 4ka which separated technically from network of Telekom by merging of SWAN and BENESTRA by green light from Slovak Antimonopoly Office since 3rd April 2018 [17]. Private label Tesco Mobile plays a role, but technically run its services technically in network of O2.

Benefits for customer as mentioned above that brings significant benefits of innovative services of Mobile operators for society with the appropriate PDP reveals In Appendix 1. Recently period was common by financial bonus for phone number transfer and mobile operators have outfight all together who will offer higher financial bonus for mobile phone transfer. Leader in past acquisition of phone transfer O2 proclaimed in September 2018 by mouth of Marketing Director Igor Tóth: “We don't want to offer bonus for phone number transfer. But if the market works with it, we have offered this bonus to customer in specified occasions. We don't want to do it, we don't like it and ideally, we wouldn't offer it. But publicly I can't promise that in any occasion we never offer bonus for mobile transfer.” As Table in Appendix reveal bonus for phone number transfer is real in offer of O2 before Christmas 2018 but customer need to ask for it, and he will gain it only as a discount from flat rates.

5. Discussion

According the right to portability settled by Article 20 in GDPR data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the origin controller. But controllers according Article 25 [18] have to implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subject.

The GDPR encourages pseudonymization for the following reasons [18]:

- Article 6 (4) (e) permits processing personal data for a purpose other than originally intended, in “the existence of appropriate safeguards, which may include encryption or pseudonymization.” Other purposes can include profiling, business analysis, outsourcing data processing to non-EU/EEA countries, and using for scientific, historical, and statistical purposes.
- Article 11 (2) exempts the Data Controller from complying with an individual's rights to access, rectification, erasure, and data portability of his or her personal data (Articles 15 – 20), if the personal data can no longer be linked to the identified individual.
- Article 25 (1) makes pseudonymization a central feature of the requirement for PDP by design and by default.
- Article 32 (1) (a) makes pseudonymization an appropriate technical measure for ensuring the security of processing personal data.
- Article 34 (1) requires that, in the event of a security breach, Data Controllers notify identified individuals impacted by the breach. Since pseudonymization data is not linked to an identified individual, notification is not required unless the individual is identifiable due to:
 - The pseudonymization key is disclosed in a security breach.
 - The individual can be identified by linking pseudonymized and additional, non-pseudonymized information (e.g., birth date, gender, zip code).
- Article 40 (2) (d) encourages the use of Codes of Conduct that include pseudonymization.
- Article 89 (1) enables processing personal data for scientific, historical, and statistical purposes if the data is safeguarded by pseudonymization.

While discussing the fact that GDPR encourage pseudonymization, we have already touched on some of, what are considered as a real difference between pseudonymization and encryption. Pseudonymization and Anonymization are two distinct terms that are often confused in the data security world. Anonymized data permanently de-links personal data from a specific identified or identifiable person. For example, personal data is encrypted and the encryption key is destroyed. As such, GDPR implementation is not required for anonymous data. To address the fact that pseudonymized data is not anonymous, the GDPR requires the following:

- Recital 26 requires pseudonymized data be treated as personal data if a specific individual can be identified “by the use of additional information.” As such, appropriate and effective technological and organization measures must be implemented to protect the pseudonymized data.
- Recital 29 requires that pseudonymized and “additional information for attributing the personal data to a specific data subject” be kept separate.
- Recital 75 requires implementing appropriate technical safeguards (e.g., encryption, hashing, or tokenization) and organizational policies to prevent unauthorized reversal of pseudonymization.

6. Conclusion

The importance of pseudonymization techniques is constantly growing in collection and processing data in digital environment. PbD as modern concept appeared in 1995, when joint Canadian-Dutch team-workers of supervisory authority created report of PETs that improve PDP. In 2009 a member of this team Ann Cavoukian formulated 7 principles of PbD lastly modified according contribution of GDPR in 2017 [21]. PETs as notion generally includes a set of computer/digital tools, applications and mechanics, that are integrated in online services and applications and evolve users, respectively subjects to protect their privacy and personal data. Nowadays professional circles in generally promote opinion, that only PETs supportive for PDP are not enough. We can conclude that evolving digital age requires a more thorough approach so-called PETs Plus, where participation of Processor is needed (as a subject that collect and process personal data for defined / settled purposes) it will have to deal with several aspects of the PDP, which should affect the proper optimization of internal processes of Processor before real collection and other use of personal data. After processing personal data mobile operators can reveal the benefits for its customers/subjects that brings innovative services for society (see App. A – processed by overview of segment of Slovak mobile operators). Operators as Data controller shall implement appropriate technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the are processed like is stated in Chapter 2 in Article (25) of Regulation [18] – especially in case of transfer the number from mobile operator to another because mobile phones as daily used device are full of personal data. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. In practice IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or processing. Up to now, tagging security or privacy features on at the end of a long production process would be fairly standard and pseudonymous data may help enable to manage PDP by requirements of PbD.

References

- [1] Baxter, Michal (2018) “GDPR promotes trust” in Data Protection Magazine AUTUMN 2018 - ISSUE 2. Data Protection World Forum [WWW Document], n.d.. Data Protection Magazine. URL <https://www.dataprotectionworldforum.com/dpmag> (accessed 12.16.18): 7 -10.
- [2] Kaczor Sebastian, Kryvinska Natalia, “It is all about Services - Fundamentals, Drivers, and Business Models” (2013), The Society of Service Science, Journal of Service Science Research, Springer, **5** (2), 2013, pp. 125-154.
- [3] Brook, Chris (2018) “Data Controller vs. Data Processor: What's The Difference?” in DigitalGuardian [WWW Document], n.d. URL <https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference> (accessed 12.26.18).
- [4] Kočíšová Lucia, Pikulík, Tomáš, Štarchoň, Peter, Šeliga, Martin (2018). “IMPACT OF GDPR ON BANKS IN SLOVAKIA - MARKETING APPROACH. PART I.” *Marketing Science & Inspirations* **13** (2): 45 - 53.
- [5] Office for Personal Data Protection of the Slovak Republic (2018) [WWW Document], n.d. URL <https://dataprotection.gov.sk/uoou/en/content/data-subject> (accessed 12.26.18).

- [6] Heywood Debbie, Pomaizlová Karin (2016) “The data protection principles under the General Data Protection Regulation” URL <https://globaldatahub.taylorwessing.com/article/the-data-protection-principles-under-the-general-data-protection-regulation> (accessed 12.27.18)
- [7] Kolah Ardi (2018) “GDPR – A QUICK SUMMARY” in Data Protection Magazine SPRING 2018 - ISSUE 1 Data Protection World Forum [WWW Document], n.d. . Data Protection Magazine. URL <https://www.dataprotectionworldforum.com/dpmag> (accessed 12.16.18): 15 -18.
- [8] Ewerlöf, Alex (2018) “GDPR pseudonymization techniques” [WWW Document], n.d. URL <https://medium.com/@alexewerlof/gdpr-pseudonymization-techniques-62f7b3b46a56> (accessed 12.15.18).
- [9] IMPERVA Data Security & Compliance Center (2018) “Pseudonymization” [WWW Document], n.d. URL <https://www.imperva.com/data-security/compliance-101/pseudonymization/> (accessed 12.26.18).
- [10] Van Schendel, Olenka (2017) “Data Masking: Anonymisation or Pseudonymisation?” [WWW Document], n.d. URL <http://digitalmarketingmagazine.co.uk/gdpr/data-masking-anonymisation-or-pseudonymisation/4666> (accessed 12.17.18).
- [11] Schien, Craig (2018) “PII (Age/Date) Blurring in IRI FieldShield” [PDF Document], n.d. URL <https://www.printfriendly.com/p/g/2DzWGz> (accessed 12.13.18).
- [12] Konečná & Zacha. Partner of eLaw.(2018) “New Slovak Data Protection Act - Exceptions to the GDPR” [WWW Document], n.d. URL <https://www.konecna-zacha.com/en/new-slovak-data-protection-act-exceptions-to-the-gdpr/> (accessed 12.14.18).
- [13] Clearwater Andrew, Theilová Zuzana (2018) “Data Privacy in 6 Steps” in Data Protection Magazine AUTUMN 2018 - ISSUE 2. Data Protection World Forum [WWW Document], n.d. . Data Protection Magazine. URL <https://www.dataprotectionworldforum.com/dpmag> (accessed 12.26.18): 14 -15.
- [14] Suchánková Lenka (2016) “Ochrana osobních údajů a bezpečnost dat - novinky v GDPR” | © forbes.com [WWW Document], n.d. URL <https://docplayer.cz/33067123-Ochrana-osobnich-udaju-a-bezpecnost-dat-novinky-v-gdpr.html> (accessed 12.27.18).
- [15] Kryvinska Natalia, “Building Consistent Formal Specification for the Service Enterprise Agility Foundation” (2012), The Society of Service Science, Journal of Service Science Research, Springer, **4** (2), pp. 235-269
- [16] 2018: European Telecommunications Network Operators’ Association”. Cit 11. december 2018. <https://etno.eu/news/etno/2018/971#>
- [17] Spectator staff “Slovakia will have a new telecom operators” [WWW Document], n.d. URL <https://spectator.sme.sk/c/20795267/slovakia-will-have-a-new-telecoms-operator.html> (accessed 12.20.18).
- [18] 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) [WWW Document], n.d. URL <http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm> (accessed 12.12.18).
- [19] Maxa, Filip (2018) “Aktuálne akcie operátorov: Pozrite si podrobný prehľad” | Živé.sk [WWW Document], n.d. URL <https://zive.azet.sk/clanok/92383/aktualne-akcie-operatorov/> (accessed 12.9.18).
- [20] Berthoty Jakub and collective (2018). “Všeobecné nariadenie o ochrane osobných údajov.” C.H. Beck, Prague, p. 285-296. ISBN: 9788074007149
- [21] Cavoukian Ann. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada (2009) [WWW Document], n.d. URL <https://www.rug.nl/research/search/research-data-office/legal/pbd/privacy-by-design-foundational-principles?lang=en> (accessed 2.13.19)
- [22] Tapp, Alan, Whitten, Ian, Housden Matthew (2014) “Principles of Direct, Database and Digital Marketing.” Harlow. Pearson Educated Limited. p. 559. ISBN: 978-0273756507
- [23] Gregus Michal, Kryvinska Natalia (2015) “Service Orientation of Enterprises - Aspects, Dimensions, Technologies”, Comenius University in Bratislava, Bratislava, ISBN: 978-8022339780.
- [24] Kryvinska Natalia, Gregus Michal (2014) “SOA and its Business Value in Requirements, Features, Practices and Methodologies”, Comenius University in Bratislava, ISBN: 978-8022337649.

Appendix A. Summary of main extra benefits in case of phone number transfers in Slovakia [19]

Mobile operator (SVK)	Orange
Bonus for number transfer	Operator offers bonus for transfer of phone numbers from competition up to 150 EUR during 20 months - for new and existing consumer. Beside discount consumer could handle and change it for another mobile data consumption.
Bonus for Orange TV	Whole season ticket for watching Champions League for 19 EUR (valid till June 2019)
Bonus 2GB of Mobile Data for group "Orange Together"	If consumer is member group "Orange Together" (up to 5 different SIM cards) he could activate benefit 2GB of Mobile Data for 6 months. If consumer would be creator of group - the consumer could benefit from extra 2GB for 12 months.
Data unlimited packages	Orange offers 4 unlimited data packages with services for fee. Consumer need to have monthly flat rate at least 15 EUR to activate it. Data consumption are through

	Apps.
Extra Mobile Data for web order	Consumer gain from Operator 2 or 5 GB of Mobile Data monthly for 1 year for web order. Volume of extra data depends on chosen monthly flat rate.
Combination of Services	If consumer chose and combine more fixed services – new consumer will automatically gain more data or TV packages for free. Actually, it is possible to use packages even though, if there is no optical network coverage.

Mobile operator (SVK)	Telekom
Bonus for number transfer	Operator offer reimbursement the contractual penalty at all or significant part of it.
Bonus for StreamOn	StreamOn Service is available up to 2 months for free, if customer choose monthly flat rate. Customers with pre-paid card have it eligible for 1 day a week to the end of year.
Bonus for Mobile Data/Flat rate	Operator added extra 10GB of Data to monthly flat rate XL for free. But cheaper flat rate programs are without extra bonuses.
Bonus for Mobile Data/Pre-paid	Packages of Mobile Data for EASY programs (pre-paid SIM), are valid for 12 months. If customer will not consume limit, this data will be transferred for another month for free.
Combination of Services	If customer have a flat rate and order a fixed service, it will be rewarded with bonus of higher variant of service for one year.

Mobile operator (SVK)	O2
Bonus for number transfer	O2 have the opportunity for 150 EUR bonus for number transfer without special promo. Customer can get 5 EUR discount for monthly flat rate for 30 months.
Mobile Data Package	O2 offers 100 GB data package through LTE network
Unlimited Flat Rate	For one single rate 20 EUR customer can enjoy unlimited calling, SMS and 0,5 GB of Mobile Data. This promo offers 96 EUR dotation for mobile phone for customer, in case of irrelevant – customer will gain extra 1 GB of Mobile Data
Bonus for Mobile Data/Flat rate	O2 offers Data Flat Rates, that are from 4 to 20 GB. Data volume depends on the customer's interest for new mobile phone tend to flat rate
Bonus for Mobile Data/Pre-paid	O2 offers for pre-paid card "O2 Freedom" 1 GB of Mobile Data for 5 EUR.
Combination of Services	Home call rates and SMS for the whole EU valid also for older flat rates called "O2 Fair". It is valid for calls, SMS and Internet at the same rates.

Mobile operator (SVK)	Tesco Mobile
Unlimited Weekly Pre-Paid	Tesco Mobile has in offer package of free minutes and SMS for 3,9 EUR/week and call after 3. minute in own network for free. Units are valid for EU and Slovakia.
Mobile Data/Pre-paid	Biggest package has 3 GB of Mobile Data and also 4G network from O2 is available.
Calls, SMS for fix rate/Pre-paid	Operator offers pre-paid card "Dot" with calls for Slovak networks for 0,039 EUR/min. Same price is for SMS. Daily internet with limit 200 MB/day is for 0,39 EUR/day.
Extra advantage	If customer charge his credit in Friday, he gains the advantage from Operator during following weekend in terms of free phone-calls in Tesco network.

Mobile operator (SVK)	4ka
Pre-Paid	Pre-paid card offers 4G LTE Network with 0,04 EUR min./SMS and 0,01 EUR/1MB of Mobile Data and call after 3. minute in own network for free
Unlimited Monthly Pre-Paid /Flat rate	O2 offers Flat Rate "Freedom ∞ +", that offers " unlimited min./SMS in whole EU and ∞ of Mobile GB. In case of overspend of actual settled rate of usage of service operator may rate 0,04 EUR for other 1 min/SMS in whole EU.
Bonus for Mobile Data	4ka offer Data package in whole EU for 2 EUR/1 GB. All Flat-rate "Freedom" are without any extra charge in EU from June 2018. In case of new card 4ka offers package "Freedom 1 Month for free" that contains 300 GB of Mobile Data in 4ka Network and 1 GB of Data in 3G network of Orange.