

Insight into PDP challenges of data transfer in wireless mobile devices

Tomáš Pikulík^{a*}, Peter Štarchoň^b

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

Abstract

Pressure for effectivity of interconnection of personal data with digital accounts eliminates paper-based personal data processing (PDP). The objective of this paper is to reveal weak spots of transfer and PDP in Wi-Fi ready mobile devices. Purpose is to reveal the set of principles for data transfer and storage of personal data in ubiquitous and pervasive network environment. Our scope is to point out the recommendation for organization (data controller) in managing data transfer procedure to prevent incidents and personal data misuse and set preventive action plan for individuals (data subject) to protect their digital accounts. The contribution of our paper is a set of recommendations that sum up principles for secure PDP that should skip individual action of data subject. The paper concludes by arguing that organization (data controller) need to manage PDP requirements and individuals (data subject) could set preventive action to protect their digital accounts. These findings provide a potential mechanism for prevent personal data - GDPR compliant methods like pseudonymization and encryption.

Keywords: *Data transfer, data privacy, pseudonymization, encryption, GDPR, ePrivacy*

1. Introduction

Deployed wireless network technologies integrate technologies and software solutions into a public benefit via open data and open access to wireless networks and applications. Development of software and pre-testing period based on wireless technology are influenced by legislation and data protection principles (e.g. consents, date of giving personal data and retention period). Data architectures need to count on possible threats like incidents and abusing personal data that have been given up to controller from subject in good faith. If we systematically think about one of the key principles of EU defined as “mobility” we should encourage and point out services that should be integrated and thoughtfully planned across wireless network technologies based on operators, geographies, and complementary modes – like transport/travel operators, events, mobile operators, banks, insurance, health-care companies, e-commerce/e-shops etc. . Results of process as trips, payments, services often and provided all in one are processed and facilitated via wireless network technologies nowadays do not need dispatch the process via physical connections, interoperable payments, and requiring combined information. Every opportunity should be taken to enhance the

connectivity of people, their devices (counting Mobile Devices and Tablets as a smartphone device) and autonomous vehicles (AVs) to the wireless networks. As market conventions emerged for mobile devices, a primary class of devices became known as personal digital assistants (PDAs). Many of these share common features, such as touch screen interfaces with color displays, linking to email and desktop software programs, and access to wireless platforms. Later, as wireless networks evolved, global manufacturers of mobile devices started to offer another class of mobile devices called smartphones, which combined the utility of a cell phone and a PDA into one device. The future of devices should inevitably result in the interconnection of mobile applications with the interconnection of the device into a mobile cloud (MC) accompanied by data transfer.

2. Data transfer challenges in the wireless network

Now, most cellphone providers offer a range of smartphones that access the Internet over a 3G or 4G wireless network. Future implementation of 5G wireless network is accompanied and face security risks associated with threats of misusing personal data and the potential integrity of individuals as common network users. Due to the proximity and upsurge of

*Tomáš Pikulík. Tel.: +421 918 713 838

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

© 2020 International Association for Sharing Knowledge and Sustainability.

DOI: 10.5383/JUSPN.12.01.003

context-aware and proximity aware applications, device-to-device (D2D) enabled mobile cloud (MC) emerging as the next step towards the future 5G system [1] and users are afraid of potential threats do not have the overall control of their personal data.

Many so-called mobile devices are not mobile as declared. It is the host that is mobile, i.e., a mobile human host carries a non-mobile smartphone device. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via wireless networks such as Wi-Fi, Bluetooth, cellular networks, near field communication (NFC). Some mobile devices can be used as mobile Internet devices to access the Internet while moving but they do not need to do this and many phone functions or applications are still operational even while disconnected to the Internet. Mark Weiser, known as the father of ubiquitous computing, computing everywhere, referred to device sizes that are tab-sized, pad and board sized,[2] where tabs are defined as accompanied or wearable centimeter-sized devices, e.g. smartphones, and pads are defined as hand-held decimeter-sized devices, e.g., laptops. Also mentioned mobility as a feature of smartphone device is confused as synonymous with having wireless connectivity, but these terms are different in depth. Not all network access by mobile users, applications and devices need to be via wireless networks and vice versa. Wireless access devices can be static and mobile users can move in between wired and wireless hotspots like public area or public transport hotspots, internet cafés, etc. [3].

What makes the mobile device unique compared to other technologies is the inherent flexibility in the hardware and also the software [4]. Flexible applications include video chat, Web browsing, payment systems, NFC, audio recording, etc. [5]. All these interactions with the provider of a network (usually mobile operator) as a controller and mobile network user (not simultaneously accessed in every single step on the wireless network) are facing security risks in personal data transfer. Processing of personal data is accompanied by various threats of personal data misuse in a sharp mode

As mobile devices become ubiquitous there, will be a proliferation of services which include the use of the cloud. The focus he is on the user and a service is the work or tasks offered and performed for the subject. More formally, the following definition is proposed [6]:

- *A service is a mechanism enabling the end-user access to one or more capabilities.*
- *A network service is service offered to the user by a network system*

With new requirements for organizations and new rights for individuals, there is no doubt that the GDPR will have a significant impact on cloud service providers that process personal data (CSP processors) [7].

2.1. Legal framework for data wireless transfer

Data privacy of EU citizens and its application for wireless network users in EU region strengthened by a common framework for data protection that is eligible and implemented by EU General Data Protection Regulation (GDPR) – European Parliament and Council Regulation No 2016/679 becoming enforceable on 25th May 2018 GDPR and afterward by the regulation of ePrivacy standards that will be implemented later (assumption in 2021). GDPR promotes trust for us as subjects and EU citizens as well [8] – 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. GDPR makes its applicability very clear – it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing is in EU or not .

The regulation about data privacy and electronic version of data regulation ePrivacy is not as well-known and familiar for the controller, processor, and users as GDPR. The upcoming ePrivacy Regulation (ePR) contains interesting transparency requirements and affects cookies, collection of metadata and has tended to stop unsolicited communication. As of now, the application scope includes electronic communications data, meta- and content data. This extends the application scope of the current ePR Directive that is still in force.

2.1.1. GDPR's close relationship with ePolicy

Both European regulations are in the same legislation package. The main reason for its occurrence is the reason for increasing the PDP, because trend heads off to too often commercialization and monetization of data even though if they are personal or not in detail. This trend is interconnected with a security risk. Mentioned regulations should come on force commonly on the 25th of May 2018 but it has not happened as was planned by the EU Commission. Final regulation of ePR is nowadays in trialogue in legislation process between officers of the European Commission, Parliament, and Council that unofficially negotiate.

Regulation of ePR is a separate regulation, that serves as an accessory of well-known GDPR. Even though regulation of ePR is already part of GDPR, ePR itself specifies certain processing of personal data. This is exactly why ePR regulation will take precedence in the field of electronic communications before GDPR regulation. In adaptation of new legislation, it is important to think about both regulations. It means that if the organization in scope of ePR you will need to adapt GDPR rules and principles too. Whereas GDPR covers data protection of user (data subjects) as individuals, ePR focus of confidentiality of electronic communication of physical persons and legal entities. Main goal of ePR is creation some kind of online letter secret. Both regulations include directly applicable rules. That principles and rules cannot be adjusted by European members by their arbitrary interests. Aim of ePR interest is to treat rapidly evolving online communication technologies and adjust legal systems of particular European members. A lot of them still don't regulate common activities at all, even though they process personal data to a large extent.

2.1.1.1 GDPR Transparency requirements

From the perspective of European data protection law, transparency is a core necessity to empower the data subject. This means knowledge and the means to hold controllers and processors of personal data accountable. For instance, it has been relatively clearly stated in recital 43 of the GDPR by explicitly mentioning transparency as a tool to better *'balance out the power asymmetry between data subjects and organizations'*. In this context, the emphasis on the empowerment of the data subject is reinforced by the explicit requirement of transparent information, communication, and modalities for the exercise of the rights of the data subject, Art. 12 (1) GDPR (bold highlights by the authors) [10]:

'1. The controller shall take appropriate measures to provide **any information** [...] 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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.'

Beyond this obligation for the controller, the GDPR has a multitude of other sources also determining that the perspective of the data subject is the deciding factor whenever it seems doubtful whether transparent information was provided about a processing operation. This is a central difference to the domain of IT security, where the processing organization, its business secrets, and company assets are the paramount subjects of protection. Therefore, in the realm of personal data protection with its fundamental rights underpinning, the following questions present themselves whenever a personal data processing operation is intended:

Data processing

Question	In which way shall the data be processed, using which means?
Operations	It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.
GDPR role	GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

Purpose limitation

Question	For which purposes shall the data be processed, and by whom?
GDPR role	The purpose for processing of personal data must be known and the individuals whose data you're processing must be informed. It is not possible to simply indicate that personal data will be collected and processed. This is known as the 'purpose limitation' principle

Data transfer and storage

Question	Is a transfer to and/or storage at other parties/foreign countries foreseen?
GDPR role	GDPR limits an organization's ability to transfer personal data outside the EU where this is based only on that body's assessment of the adequacy of the protection afforded to the personal data

Data extension

Question	Which data shall be collected and processed, and to which extent?
GDPR role	GDPR extension is designed to help online stores comply with the latest legislative EU requirements and strengthen the data security

2.2. Secure transfers and PDP challenges

The Near Field Communication (NFC) technology has security features that help in making secured financial transactions. Besides M-commerce, an increasing variety of equipment and devices integrate near field communication such as cars, washing machines, cookers, vending machines, televisions, speakers, headsets, cameras, tablets, and laptops.

2.3. 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 defines the role of the data controller, data processor, and the 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 the processing of personal data. A data processor simply processes any data that the data controller gives them on behalf of the data controller. The data processor does not own the data that they process nor do they control it. The data processor will not be able to change the change the purpose and how the data is used. Furthermore, data processors are bound by the instructions given by the 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 [11]. On the other hand, GDPR set also new principles of PDP. The data subject is any natural person, whose personal data are regarded. For clarification, Personal Data is a name, an identification number, location data, an online identifier or 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 [12]. An only individual natural person may be considered as data subject regardless of his citizenship. There is no way to consider the legal person as a natural person. The same applies to natural persons – entrepreneurs while acting within their business activity [13]. This poses one significant requirement on the framework, apart from the already discussed ones - that GDPR as a new framework for unit 500 million of customers has strengthened and unite the aspect of data privacy that retaining the main principles of previous Data Protection Directive 95/46/EC. The core rules seem well-known and familiar for experienced data specialists (e.g. experienced data practitioners before defining the position of Data Privacy Officer by Article 20 in specified cases not only for the controller but for processor). Regulation brings by its hidden traps, there are also many important new obligations in coherence with a tougher regime of data privacy in terms of usage of fines and sanctions for the unwary ones. The aim is to strengthen the 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.

Table 1. Data protection principles according to GDPR

Lawfulness, fairness, and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner concerning 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 minimization	Personal data shall be adequate, relevant and limited to what is necessary concerning 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 the 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

2.3.1. Overview of the benefits of data transfer - Slovak MNO

We have mapped this situation and potential benefit for transfer 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 a relevant fact on our local market because more than 200 000 people transfer their mobile phone number to another mobile operator every year (comparable in 2017 and 2018). Slovakia has a specific situation where the market is divided for big three - Orange, Telekom, O2 and challenged by national Slovak Operator 4ka which separated technically from a network of Telekom by merging of SWAN and BENESTRA by green light from Slovak Antimonopoly Office since 3rd April 2018 [14]. Private label Tesco Mobile plays a role but technically runs its services technically in a network of O2.

Benefits for a customer as mentioned above that bring significant benefits of innovative services of Mobile operators

3. 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 [10] 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.

GDPR encourages pseudonymization for following reasons:

- 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,

for society with the appropriate PDP reveals In Appendix 1. Recently period was common by financial bonuses for phone number transfer and mobile operators have outfought all together who will offer higher financial bonus for mobile phone transfer. A leader in the past acquisition of phone transfer O2 proclaimed in September 2018 by the mouth of Marketing Director Igor Tóth: “We don’t want to offer a bonus for a phone number transfer. But if the market works with it, we have offered this bonus to the customer on 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 on occasion we never offer a bonus for mobile transfer.” As Table in Appendix reveal bonus for phone number transfer is real in the proposition of O2 before Christmas 2018 but the customer needs to ask for it, and he will gain it only as a discount from flat rates.

and data portability of 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 encourages pseudonymization, we have already touched on some of, what

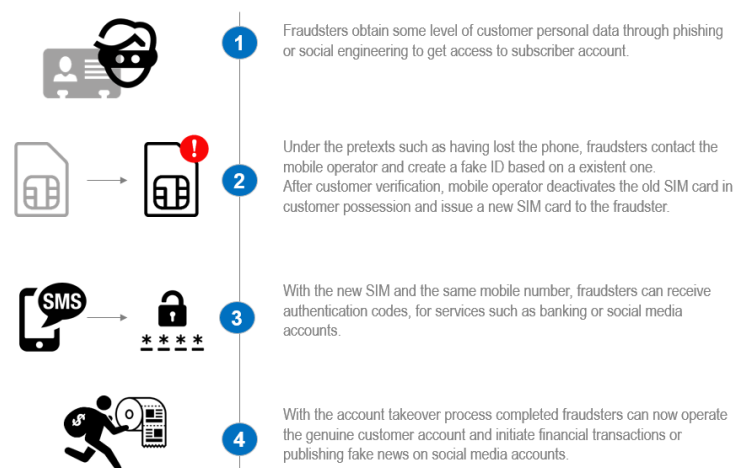
is considered as a real difference between pseudonymization and encryption. Pseudonymization and Anonymization are two distinct terms that are often confused in the data security world. Anonymized data permanently de-links personal data from a specific identified or identifiable person. For example, 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 to 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 organizational 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.

NFC and its data speed and transfer capacity are other facets of the technology as it provides ten times faster data transfer, which is also estimated to boost the market growth. This technology is expected to gradually replace traditional transaction services which are expected to favor the NFC market growth. Otherwise, the usage of wireless technology and smartphones and features like NFC for transactions could bring threats like SIM swapping. SIM swapping involves a hacker duping the user’s cell provider into believing that you’re activating your SIM card on another device. In other words, hackers are stealing your phone number and associating it with their SIM card. If successful, this attack will deactivate your device, and their device will become the destination for all texts, phone calls, data, and accounts tied to your phone number and SIM card. With that information, the attacker could easily gain access to your app accounts, personal data, and financial information. They could even lock you out of your services (see Figure 1)

Figure 1:SIM swapping fraud scheme [15]



Source: wedotehnologies.com

3. Conclusion

The importance of pseudonymization techniques is constantly growing in collection and processing data in digital environment. PbD as a 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 [15]. 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 collects 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 bring innovative services for society (see App. A – processed by an overview of a 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 are processed like is stated in Chapter 2 in Article (25) of Regulation – 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, the IT department, or any department that processes

personal data, must ensure that privacy is built into a system during the whole life cycle of the system or processing. Up to now, tagging security or privacy features at the end of a long production process would be fairly standard and pseudonymous data may help enable to manage of PDP by requirements of PbD.

Recommendations to avoid the incidents in data transfer in a wireless network should include:

- (i) Develop wireless network policies
- (ii) Conduct risk assessments to determine the required level of security
- (iii) Limit access to wireless networks through the use of wireless security measures [12]
- (iv) Maintain logical separation between wireless and wired networks
- (v) Perform wireless scans to identify wireless networks and applications (on a regular base)
- (vi) Enforce wireless network policies

Many significant consequences than incidents in PDP are waiting for users in case of real misuse of personal data in data transfer (should possibly occur in case of phone number transfer) as a SIM Swap attacks. Fraud person will gain the personal information of person from different ways like fake call, SMS, email, link, social media, etc. mobile number is linked with bank card the fraud person will gain the access of Bank account, credit card number and other PII easily by trying various methods like MNC, Phone call, Hacking. It is difficult to undo the damage that occurs.

Recommendations for preventing the SIM swap attacks are:

- (i) Beware of a phishing scam
- (ii) Reduce excessive personal data online
- (iii) Protect accounts

To put recommendations in details:

- (i) Avoid to click links, download programs, or sign in to websites that user does not recognize
- (ii) In addition to phishing as the early part of a SIM swap involves **social engineering** - basically collecting as much data about user (data subject) as possible so the hacker can reliably pass for user (data subject) over the phone or via email
- (iii) Many digital accounts have settings that can help user takes back his accounts if they're ever stolen - but they need to be properly set up before the account is stolen in order to be of any help. These small steps should help to be a huge step ahead from attackers:
 - a. Set **PIN number** that is required for logins and password changes
 - b. Rely on a **suitable two-factor security method** that depends on a physical device, like Google

Authenticator or Authy, rather than SMS-based verification for login

- c. Set up strong answers **security recovery questions** that aren't tied to your personal information
- d. Unlink smartphone phone number from user accounts, where possible (User could always use a free **Google Voice number** if is it required to have one for your sensitive accounts)
- e. Generate long, randomized, and **unique passwords** for each account
- f. Use an **encrypted password manager**
- g. Don't use your favorite services (Google, Facebook, et cetera) to sign in to other services; all an attacker needs is to break into one to have access to a lot more of your digital life.
- (iv) User should also make note of important account-related information that could be used to identify the rightful account holder, such as:
 - a. The month and year you created the account
 - b. Previous screen names on the account
 - c. Physical addresses associated with the account
 - d. Credit card numbers that have been used with the accounts or bank statements that can confirm you were the one who made purchases
 - e. Content created by the accounts, such as character names, if the account is for an online video game

Future research should consider the potential effects of more consistent interconnection digital accounts with personal data especially in both future challenges:

- (i) ePR (assumption of application in 2021)
- (ii) process of certification and re-certification for ISO 27001 (information security standard, part of the ISO/IEC 27000 family of standards)

Future investigations are necessary to validate the kinds of conclusions that can be drawn from this study. Future studies could investigate the association between data privacy standards across interests of mobile network operator's association (like GSMA, EENA, ETNO etc.) focusing on other challenges for ubiquitous and pervasive networks environment like Digital Identity & and mobilizing the Internet of Things. This may be considered a further validation of the data transfer requirements in changed environment.


Acknowledgments


We would like to thank to ANT-19 conference committee, Acadia and International Association for Sharing Knowledge and Sustainability for the Special Issue Invitation for Special Issue in the International Journal of Ubiquitous Systems and Pervasive Networks (JUSPN) to the possibility to extend the paper by new materials.


Nomenclature


3G, 4G, 5G	Mobile data networks
AVs	Autonomous vehicles
CSP	Cloud service providers
D2D	Device-to-device
EEA	European Economic Area
EU	European Union
ePR	ePrivacy
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)
MC	Mobile cloud
PbD	Privacy by Design
PDP	Personal Data Protection
PDA	Personal digital assistant


Appendix A. Summary of main extra benefits in case of phone number transfers in Slovakia [16]

Mobile operator (SVK)	Orange 
Bonus for number transfer	The operator offers a bonus for the transfer of phone numbers from competition up to 150 EUR during 20 months - for new and existing consumers. Beside discount consumers could handle and change it for another mobile data consumption.
Nonstop packages	The operator added to offer 6 unlimited packages of selected service for a fee. Consumer needs to have a monthly flat rate of at least 15 EUR to activate it.
Orange Love: Combination of services	If the consumer chose and combine more fixed services – new consumers will automatically gain more data or TV packages for free. It is possible to use packages even though if there is no optical network coverage.
Extra Mobile Data for web orders	Consumer gain from Operator 2 or 5 GB of Mobile Data monthly for 1 year for web order. The volume of extra data depends on the chosen monthly flat rate.
4G Internet at home	The operator offers 3 packages. Service is available for more than 90% of households. The faster package is not always available in the whole coverage area

Mobile operator (SVK)	Telekom 
Bonus for number transfer	The operator offers reimbursement for the contractual penalty at all or a significant part of it.
Bonus for StreamOn	StreamOn Service is available if customer choose monthly flat rate
Bonus for Mobile Data/Flat rate	The operator added an 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 the customer will not consume limit, this data will be transferred for another month for free.
Combination of Services	If a customer has a flat rate and order a fixed service, it will be rewarded with a bonus of a higher variant of service for one year.

Mobile operator (SVK)	O2 
Bonus for number transfer	O2 has the opportunity for a 150 EUR bonus for number transfer without a special promo. Customer can get 5 EUR discount for a monthly flat rate for 30 months. The operator offers reimbursement for the contractual penalty at a maximum high of 150 EUR.
Mobile Data Package	O2 offers 100 GB data package through LTE network
Extra Bonus for everyone	It is possible to gain extra 5GB of Mobile Data for free in application of provider
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 the Internet at the same rates.

Mobile operator (SVK)	Tesco Mobile 
Unlimited Weekly Pre-Paid	Tesco Mobile has an offer package of free minutes and SMS for 3,9 EUR/week and calls after 3. minute in own network for free. Units are valid for EÚ and Slovakia.
Mobile Data/Pre-paid	The biggest package has 3 GB of Mobile Data and also 4G network from O2 is available.
Calls, SMS for fix rate/Pre-paid	The operator offers pre-paid card "Dot" with calls for Slovak networks for 0,039 EUR/min. The same price is for SMS. Daily internet with limit 200 MB/day is for 0,39 EUR/day.
Extra advantage	If customer activate the application for consumption control, he will gain extra 1,47 GB of Mobile Data for one month

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 the case of overspend of the actual settled rate of usage of service, the operator may rate 0,04 EUR for the other 1 min/SMS in the whole EU.
Bonus for Mobile Data	4ka offer Data package in whole EU for 2 EUR/1 GB. All Flat-rate "Freedom" is without any extra charge in EU from June 2018. In the case of the 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 a 3G network of Orange.

References

- [1] Ashraf MI, Tamoor-ul-Hassan S, Shahid M, Tsang KF, Rodriguez J. Device-to-Device Assisted Mobile Cloud Framework for 5G Networks. Proceedings of the 14th International Conference on Industrial Informatics. Sponsored by: IEEE Industrial Electronics Society and Prime Institute, Futuroscope-Poitiers, France, 2016. <https://doi.org/10.1109/INDIN.2016.7819312>
- [2] Weiser M: The Computer for the Twenty-First Century. Scientific American, 1991. Volume-265 | Issue-3: pp. 94–104. doi:10.1038/scientificamerican0991-94. <https://doi.org/10.1038/scientificamerican0991-94>
- [3] Poslad S: Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction. Wiley, 2009. ISBN 978-0-470-03560-3
- [4] 802.11 Wireless LAN, IEEE standards, www.ieee.org
- [5] Beddall-Hill N; Jabbar A, Al Shehri, S: Social Mobile Devices as Tools for Qualitative Research in Education: iPhones and iPads in Ethnography, Interviewing, and Design-Based Research. Journal of the Research Center for Educational Technology. Volume-7 | Issue-1, pp. 67–90. ISSN 1948-075X.
- [6] Nor Shahniza Kamal Bashah, Kryvinska N., Do van Thanh: Service Discovery in Ubiquitous Mobile Computing Environment [accessed Aug 30 2019]. Conference paper iiWAS'2010 - The 12th International Conference on Information Integration and Web-based Applications and Services, 8-10 November 2010, Paris, France. doi:10.1145/1967486.1967609 <https://doi.org/10.1145/1967486.1967609>
- [7] Webber M: The GDPR's impact on the cloud services provider. PDP Journal's Privacy and Data Protection Volume-16 | Issue-4 pp 11 - 14 See: <http://www.pdpjournals.com> (accessed 20.18.2019).
- [8] Baxter, M: GDPR promotes trust. In Data Protection Magazine AUTUMN 2018 (Issue 2). Data Protection World Forum, 2018 [www document], n.d.. Data Protection Magazine. <https://www.dataprotectionworldforum.com/dpماغ> (accessed 12.16.18):pp 7 -10.
- [9] Kočišová L, Pikulík, T, Štarchoň, P., Šeliga, M. (2018): Impact of GDPR on banks in Slovakia - Marketing approach. Part I." Marketing Science & Inspirations 13 (2): 45 - 53.
- [10] Schlehahn E, Wenning R.: GDPR Transparency Requirements and Data Privacy Vocabularies. In: Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (eds) Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, vol 547. Springer, Cham. https://doi.org/10.1007/978-3-030-16744-8_7. ISSN 978-3-030-16744-8 (online)
- [11] Brook, Ch: Data Controller vs. Data Processor: What's the Difference? in DigitalGuardian, 2018 [www Document], n.d. URL <https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference> (accessed 21.18.2019).
- [12] 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 21.8.2019).
- [13] Office for Personal Data Protection of the Slovak Republic (2018) [WWW Document], n.d. URL <https://dataprotection.gov.sk/uouu/en/content/data-subject> (accessed 21.18.2019).
- [14] Spectator staff “Slovakia will have a new telecom operator” [WWW Document], n.d. URL <https://spectator.sme.sk/c/20795267/slovakia-will-have-a-new-telecoms-operator.html> (accessed 12.20.18).
- [15] Cavoukian A.: 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 22.8.2019) <https://doi.org/10.31142/ijtsrd23982>
- [15] Awale SM, Prave G.: Awareness of Sim Swap Attack Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.995-997, URL: <https://www.ijtsrd.com/papers/ijtsrd23982.pdf>
- [16] Maxa, Filip (2019) “Aktuálne akcie operátorov: Pozrite si podrobný prehľad” | Živé.sk [WWW Document], n.d. URL <https://zive.azet.sk/clanok/92383/aktualne-akcie-operatorov/> (accessed 22.8.2019).