Assessing General Data Protection Regulation for Personal Data Privacy: is the End of "Take it or Leave it" Approach for Downloading Apps?

Spyros E. Polykalas
Department of Digital Media & Communication
TEI of Ionian Islands
Argostoli Kefalonia, Greece
email: s.polykalas@teiion.gr

***Abstract*—On a daily basis, an enormous amount of data are generated from several personal and non-personal devices, such as mobile phones, tablets, computers, sensors for the Internet of Things applications, etc. In most cases, the data are stored and analyzed aiming to improve the quality of the provided services. In cases, where these data are correlated, directly or indirectly, with a person are characterized as personal data. The collection, storage and processing of personal data raise several issues on personal data privacy, in particular when users are not well informed regarding the processing of their personal data. The aim of this paper is to examine to what extent the procedures currently followed in one of the most popular personal applications stores (Google Play), which contains more than 3 million mobile applications including social media applications, are in compliance with the provisions of the General Data Protection Regulation (GDPR). Our analysis shows that the current procedures, followed by Google Play store, are not fully in compliance with the upcoming framework, in particular with issues related to, users awareness regarding the scope of personal data process, non availability of user option to install an app without giving full access to his/her personal data and protection of minor users. It is argued that several modifications should be done, both from apps developers and stores, in order to harmonize the relevant procedures with the provisions laid out in the upcoming EU Regulation.**

Keywords- data privacy; personal data; GDPR; Google Play store; Android; EU framework.

I. INTRODUCTION

World is moving in fully digitalized societies, where citizens are using electronic communication services, mainly internet based, for entertainment, communication and work. Most of us, are always connected to internet with personal devices, such as smartphones in which several applications (apps) are installed. The increased demand for personal apps leads to the development of millions of apps, which are available for downloading in internet app stores, such as Google Play store. The vast majority of these apps require access to data, stored in users devices, which directly or indirectly could lead to personal identification, therefore are characterized as personal data. Indeed, as shown in [10] the majority of the examined mobile applications (84%), require access to almost every single file stored in mobile devices, while users are evaluating mobile applications, without taking into account the level of data access, requested by each mobile application. That leads to a preliminary conclusion that users, either are not aware about the level of required data access by mobile applications, or they choose to install mobile applications, regardless of the length of the required data access.

The framework of personal data and personal privacy remained the same in European Union (EU), for almost two decades. After four years of public consultations and discussions, within EU [8], in 2016 the General Data Protection Regulation (GDPR) was approved by the European Parliament, aiming to protect users from collecting, storing and processing of their personal data. The upcoming EU Regulation, introduces new principles to several issues related to personal data privacy in electronic communication sector, such as, the fully awareness of user about the purpose of personal data collection, the obligation of the existence of user consent, prior the personal data storage and process, the protection of minor users personal data introducing as mandatory the existence of parental consent, and several other issues.

Currently, the majority of internet stores and personal apps follow a "take it or leave it" approach, which means that users are not allowed to restrict or minimize the extent of the required personal data access, prior the installation of the selected app in their personal devices. If a user wants to download and install an app, has to accept the full set of personal data access types, determined by app developer, even though some of the required personal data types are not necessary for the provided app running, at least with the basic functionality. The scope of this paper is twofold: first, to designate the main principles, laid down in the GDPR, in relation to protection of user personal data privacy, when a user downloads an app to his/her personal device and second, to examine whether the procedures and principles currently followed by internet app stores and by app developers are in accordance with the relevant principles contained in the GDPR. To do so, one of the most popular internet app store was chosen (Google Play store) and an indicative, free of charge, popular personal app was selected ("Temple Run 2"). It should be noted that the scope of this paper is not to criticize the procedures, followed by the selected app, but to examine in general the harmonization of the principles followed in Google Play store, by millions of apps, with the provisions of the forthcoming Regulation. In this context, it models the relevant procedures contained in the GDPR and compared them, with the current procedures followed by Google Play store, in order to determine the

 ISBN: 978-1-61208-595-1

GDPR provisions that are violated by the procedures currently followed in Google Play store.

The rest of this paper is organized as follows: in Section II, a literature review is discussed, while in Section III, first are modeled the procedures laid down in the GDPR and then are compared with the relevant procedures, in relation to personal data collection/storage/processing, followed by Google Play store. Finally, in the last section, the findings of this paper are discussed.

.

II. LITERATURE REVIEW

The issues of personal data protection and in general data privacy, have drawn the attention of several researchers. The majority of existing research deals with the awareness of users in relation to the extent of personal data access, development of applications for personal data management, type of personal data that apps shared with third parties, sufficiency of information provided by app developers in relation to purposes of personal data collection and several other issues. In particular in [5], researchers concluded that the majority of apps does not provide sufficient information to users, in relation to the purposes and necessity of personal data collection. In addition they found that for 31% of the examined apps, the requested types of personal data access is excessive in relation to the apps functionality. In another study [6], researchers developed an app permission manager that showed users nudges about the data handling performed by the installed personal apps. They concluded, that a large percentage of users, given the right information, will modify the permissions initially granted to the apps in their smartphones. In [7], users were paid, in order to assert their level of comfort, with respect to giving apps access to privacy-related information in their smartphone. Researchers concluded that users, have different expectations compared to the developers of the applications, moreover they find it difficult to assess, why an app may require certain privacy-related data. In addition, it was found that when users are properly informed, then they feel more comfortable in providing access to the required information.

As regards, the compliance of the framework in relation to protection of personal data privacy, researchers are focused on minors protection, user consent, portability of personal data and several other issues. More specific, in [1] researchers critically assess the provisions of the new EU Regulation, related to the consent of minors, and makes a comparative analysis with the requirements stipulated in the relevant framework in the USA, in order to identify pitfalls and lessons to be learnt before the new rules in the EU become applicable. In [2], they discuss the provisions of new EU Regulation, in relation with the associated data protection and user privacy concerns, making reference to such Internet of Things (IoT) service offerings, as smart retail, the smart home, smart wearables, smart health devices, smart television and smart toys. In [3], researchers deal with a new obligation introduced by the GDPR, in relation to personal data portability. As personal data portability is defined the user right firstly, to receive his/her personal data, which he/she has provided to service provider, such as web service provider, and secondly, to transmit those data to another provider without hindrance from the controller to which the personal data have been initially provided. The researchers suggest that, in order to ensure comprehensive data portability that reaches out to all relevant stakeholders, including businesses, the provisions in the GDPR need to be analyzed by taking into account EU competition rules. Another interesting approach is related to the provisions included in the GDPR, in relation to the requirements and the implications put in place for the design of learning analytics systems [4].

III. GDPR AND GOOGLE PLAY STORE

A. Modelling the main GDPR provisions

The new EU Regulation published in 2016, introduced a new framework at EU level in relation to users personal data privacy. The provisions included in the new Regulation, are aiming to protect users' personal data, taking into account the digitalized environment of our societies. The scope of this study is to examine the provisions of the new Regulation, in relation to the principles that should be followed by app stores and developers, in relation to user awareness regarding the personal data protection. In addition a comparative analysis is made between the provisions included in GDPR and the relevant, followed by app developers and Google Play store.

In the following paragraphs are analyzed the main relevant provisions of the Regulation in relation to personal data privacy.

First of all, the scope of the GDPR (article 1) is related, among others, to the protection of natural persons (hereafter users), regarding the processing of personal data, regardless of whether the storage and processing of personal data take place in the EU, or not. As personal data (article 4), are considered all information relating to an identified or identifiable user, such as name, location data, an online identifier, etc. The principles, in relation to personal data collection/storage/processing, should be characterized by lawfulness, fairness, transparency, purpose limitation and data minimization (article 5). Purpose limitation means, that data shall be collected and processed for specified, explicit and legitimate purposes and not further processed is permitted, in a manner that is incompatible with those purposes. Data minimization means that collected and processed data, shall be adequate relevant and limited to what is necessary, in relation to the purposes for which they are processed. In addition the process of personal data is lawful, only if and to extent, the users have given consent for the processing (article 6). It should be noted that there are few more cases, in relation to the lawfulness of personal data processing, where user consent is not required such as, protection of user vital interest, performance of user contract, etc., but these issues are out of the scope of this paper. In article 7 of the Regulation, are contained the conditions for user consent. First of all, the controller of personal data (in our case, Google Stores and app developers), shall be able to demonstrate that the user has consented to personal data

 ISBN: 978-1-61208-595-1

processing, when personal data processing is based on user's consent. In addition in cases, where users have given consent, in the context of a written declaration which also includes and other matters, the request of consent shall be presented in a manner, which is clearly distinguishable from the other matters, in a intelligible and easily accessible form, using clear and plain language. In order to assess, whether the consent has been given in a freely manner, utmost account shall be given, whether the provision of a service is conditional on content to the personal data, that are not necessary for the provision of the service. Last but not least, it should also be pointed out, that the Regulation introduces new provisions in relation to the collection and process of minors' personal data. In particular in article 8, it is mentioned that in case that user is under 16 years old, then the collection/storage/processing of his/her personal data, in relation to the provision of a service, is lawful, only if and to the extent that the consent has been given, or authorized, by the person who has the parental responsibility over the child.
In the following figure (Figure 1), are modeled the procedures that shall be followed when a user is downloading an app, to his/her personal device, according to GDPR provisions.

The first step, is related to whether the provision of an electronic communication service, concerns the collection and process of personal data. In the case, that the provision of a service is related with personal data collection, then the next step deals with the user consent. In particular, in the case that user has not give his/her consent, for the collection/process of his/her data, then the whole procedure is incompatible with the provisions of GDPR. In case, that user is under 16 years old, then the consent of the person, who has the parental responsibility over the minor user, is required otherwise the whole process is unlawful. In case, that user has give his/her consent, then it is crucial to examine, whether user has been informed about the purpose of personal data collection and process. If user is not aware about the purpose, then again the whole process is not compliant with GDPR provisions. The next step is dealing with the principles of data collection/processing, which shall follow the rational of purpose limitation and data minimization. For example, if data are collected / processed only for reasons relevant to service provision, then the collection of personal data, for advertising reasons is not lawful. In addition, if personal data are collected, which are not necessary and relevant to the informed purposes, then the whole process is not compliant with the provisions of GDPR. In the case, that user consent related to collection/processing of personal data, has been given within the context of other matters, such as, the terms and conditions of an offered service, then the request for personal data, shall be clearly distinguished from the other matters. Last but not least, it should be examined whether the user has the option to receive the requested service, but at the same time to deny the collection and process of his/her personal data, that are not necessary for the provision of the service.

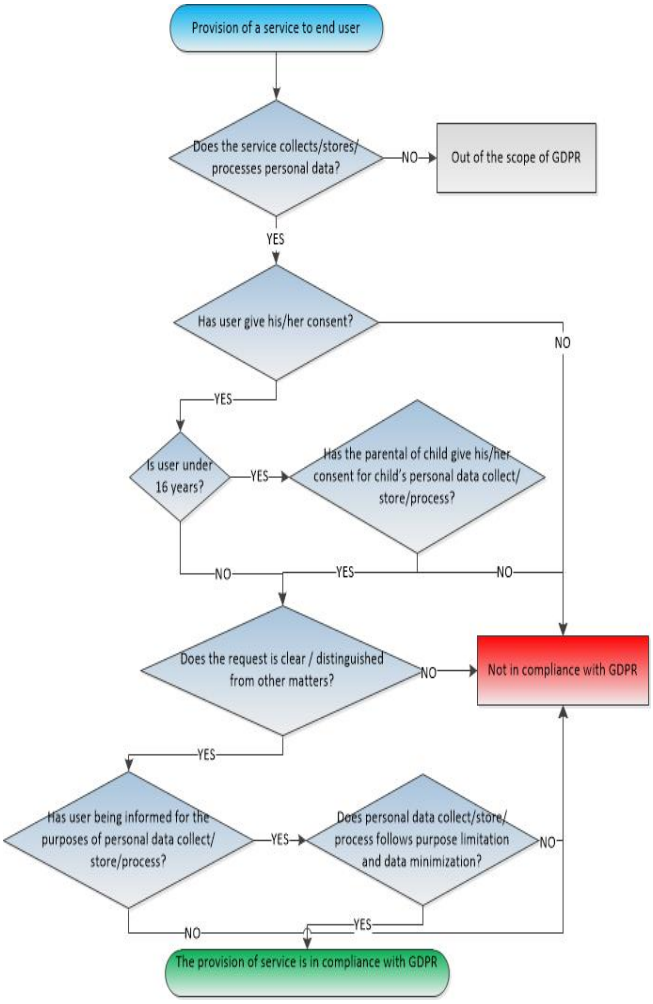

Figure 1. Main GDPR personal data privacy provisions during an app downloading.

B. *Downloading an app from Google Play store*

In the next paragraphs, the current procedure followed in Google Play store for downloading an application, is described. Google Play store is organized in four main categories: Apps, Movies, Music and Books. The Google Play store, contained (June 2016) more than three million mobile applications grouped in the following three main categories: the first one which contains 28 sub-categories, the second titled Games, contained about 17 sub-categories and the third one named Family contained about 9 sub-categories. Each sub-category contained hundreds or thousands mobile applications available for downloading either, free of charge or, paid. A precondition to download an app, from Google Play store, is the existence of a subscription to Google services and a personal device running Android operating system. It should be noted that subscription to Google services is allowed to a user, which is older than 13 years old (at EU level). In order to analyze the steps required for the installation of a Google Play application, one free of charge popular mobile app was

 ISBN: 978-1-61208-595-1

selected and installed, named "Temple Run 2", which up to June 2017 had more than 100M installations. It should be noted that we logged in, with an account of a 15 years old user. The user of Google Store has the option to click the button "install", or before that, has the option to scroll down the page, in order to get information for several issues including the "Permissions", required by the app, as well as, the "Privacy Policy" of the app developer. By clicking "view details", under the header of "Permission", user is informed about the access, required prior the installation of the app. For the selected app user is informed, that the app will have access to "in app purchase", "photos/media/files", "storage", "view WiFi connection information", "view network connections" and "full network access". According to the explanation, given by app developer, "app purchase" means that the app may ask the user to make purchases inside the app, while access to "photos/media/files" means, that the app will be able to read, modify or delete the content of usb storage. The same explanation is given, by the app developer, in relation to access to "storage". The potential categories of permissions, required by any app in Google Store, are categorized and explained by Google Store site, in the terms and conditions of Google Store. The following table compares, for each permission category required in the selected app, the relevant description provided by the selected app, and Google Play store.

TABLE I. DESCRIPTION OF THE REQUIRED PERMISSIONS

Type of access	**Description / Explanation**	
	Google Play store	***Selected App***
In-app purchases	An app can ask you to make purchases inside the app.	not explained
Photo / Media / Files	An app can use files or data stored on your device. Photos/Media/Files access may include the ability to:Read the contents of your USB storage (example: SD card), Modify or delete the contents of your USB storage, Format external storage, Mount or unmount external storage.	read the contents of your USB storage modify or delete the content of your USB storage
WiFi connection information	An app can access your device's Wi-Fi connection information, like if Wi-Fi is turned on and the name(s) of connected devices. Wi-Fi connection information access may include the ability to view Wi-Fi connections.	view WiFi connections
Other	Other types of acces such as receive data from internet.	view network connections full network access
Storage	NA	read the contents of your USB storage modify or delete the content of your USB storage

It is obvious that the explanation given, by the selected app, is more generic and less specific than those included in the Google Store privacy policy, while it was expected the opposite. In addition, it was expected that the explanation provided by a specific app, will be easily understandable using plain and clear language.

C. Comparative analysis

Coming back to the awareness and understanding of a user, who is willing to download the selected app, an intermediate user is not aware what does mean "access to USB storage". The first question that may come in his/her mind is "does my phone has a USB connection / capability?". The vast majority of intermediate users correlates the "USB connection" with the memory USB sticks, used in laptops and desktops as external disks. So this kind of explanation, may confuse users, rather than assist them to understand the purpose, scope and type of the required permission. From an expert user point of view, all these required types of permissions arise several additional reasonable questions such as "for what reasons an app game requires, as a precondition for the installation, full access to all files stored in my personal device?". Furthermore, several other reasonable questions may arise for expert and non-expert users such as: "Do all these required permissions are necessary for the running of the app?" or "Can the app run, even with limited capabilities, if users deny the access to the full range of the required permissions?". Regarding the last question we did the following test. After downloading the app, an option, provided by Android operating system, was used to view and modify the permissions given in each app, installed in a personal device. So, the initial permissions of the selected app were modified, by reducing the permission related to "Photo/Media/Files". The app was still running, in the personal device, without noticing any limitation to the app functionalities / capabilities. So, a new important question arises: "why all these permissions are set as precondition for app installation, since are not necessary for the app basic functions?".

Coming back to the options, that a Google Play user has prior the installation of an app, we noticed that a user hasn't the option to install an app, without giving full access to all required permissions by an app. To our understanding a phrase that can perfectly describe the practice currently followed by app stores and millions of personal app developers, is "take it or leave it" approach.

The above analysis reveals discrepancies between the current approach, followed by millions of apps in Google Store, with the relevant principles, laid down in the forthcoming GDPR Regulation, as regards the personal data privacy. In particular, it was shown that the current followed practices, are in contrast with the provisions of the EU Regulation, in relation to the protection of minors' personal data. As described above a minor user (15 years old) is able to download and install an app, which requires access to his/her personal data (access to stored files in the device), without the consent of the person who has the minor's responsibility. This is fully incompatible with the provisions of EU Regulation. In addition, the selected app requires, as

 ISBN: 978-1-61208-595-1

precondition for downloading and installation, access to personal data that, as proved, are not necessary for the running of the selected app, at least with the basic features of the provided app. Furthermore, we noticed that the description provided by Google Play store and the developer of the selected app, in relation to the required access to user's personal data, is generic without providing to user a clear, specific and understandable explanation, in relation to the purpose, as well as, the extent of personal data access.

IV. CONCLUSIONS

This paper assesses to what degree the current procedures, followed by Google Play store, are in compliance with the provisions of the General Data Protection Regulation, in relation to personal data. It was critically examined issues such as, the existence of user consent for personal data access, protection of minor users, existence of specific and understandable explanation, in relation to the types of personal data access and the clarification of the purposes for which access to personal data is required. Furthermore, focus was given to the procedures that should being followed by a user, who is willing to download and install a mobile app to his/her personal device. To do so, an app was selected from Google Play store app and downloaded / installed in a personal device.

The findings of this paper reveal incompatibilities between the new EU Regulation (GDPR) and the procedures currently followed in one of the most popular personal app store (Google Play store). In particular, the currently followed approach, we call it "take it or leave it" approach, does not allow users, to download and install a personal app without, prior the installation, giving full access to all, required by app developer, set of personal data. This approach is not compliant with the provisions of the GDPR. Furthermore, users are currently not well informed, neither for the purposes of the required personal data access, either for the extent of required access. Another important incompatibility deals with the protection of minors and the requirement set by new EU Regulation, regarding the mandatory existence of parental consent, in case, an app requires access to children's personal data.

It is argued, that the current Google Play store procedures, failed to be in accordance with the new EU framework, which requires that users of electronic communication services, need to be fully aware about the purposes of personal data selection and the extent of personal data access. In addition users shall have simple tools in order to understand how their privacy can be compromised and have the means to deny the use of their personal data, or to minimize the extent of personal data access.

Further research could be done in relation to the procedures followed by other popular stores, like IOS store, as well as, to examine several other indicative apps in order to verify or not, the findings of this paper.

REFERENCES

[1] M. Macenaite, and E. Kosta, "Consent for processing children's personal data in the EU: following in US footsteps?", Information and Communications Technology Law, pp.146-197, May 2017. DOI=10.1080/13600834.2017.1321096.

[2] A. Chaudhuri, "Internet of things data protection and privacy in the era of the General Data Protection Regulation", Journal of Data Protection & Privacy, vol. 1, pp. 64-75, December 2016.

[3] A. D. Vanberg and M. B. Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", in European Journal of Law and Technology, vol. 8, 2017. [Online]. Available from http://ejlt.org/article/view/546/727 (2017.08.04).

[4] T. Hoel, D. Griffiths and W. Chen, "Implications of the European Data Protection Regulations for Learning Analytics Design", Learning Analytics and Knowladge (LAK 2017), ACM, Mar. 2017, pp. 243-252, ISBN: 978-1-4503-4870-6.

[5] Office of the Privacy Commisioner of Canada, "Results of the 2014 global privacy enforcement network sweep", (September 2014). [Online]. Available from https://www.priv.gc.ca/media/nrc/2014/bg 140910 e.asp (2017.08.04).

[6] H. Almuhimedi, et al., "Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging", In Proceedings of the 2015, ACM, Conference on Human Factors in Computing Systems (CHI 2015), ACM, pp. 787-796. ACM, New York, NY, USA, 787-796. DOI=https://doi.org/10.1145/2702123.2702210.

[7] J. Lin, et al., "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing", In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12), ACM, New York, NY, USA, pp. 501-510, 2012. DOI=http://dx.doi.org/10.1145/2370216.2370290.

[8] P. D. Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", Computer Law & Security Review, vol. 28, pp. 130-142, April 2012.

[9] Statista: The statistical portal [Online]. Available from: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/ 2017.08.03.

[10] S. Polykalas, G. Prezerakos, F. Chrysidou and E. Pylarinou, "Mobile apps and data privacy: when the service is free, the product is your data", In Proceedings of the 2017 International Conference on Information Intelligence Systems Applications (IISA 2017), IEEE, Larnaca, Cyprus, 2017, in press.

 ISBN: 978-1-61208-595-1