EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions

EDPS

November 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

These Guidelines focus on the processing of personal data through mobile applications developed and distributed under the control of EU institutions and bodies. As these mobile applications could process personal data, including sensitive categories, respecting data protection principles is very important.

Mobile applications use the specific functions of smart mobile devices like portability, variety of sensors (camera, microphone, location detector…) and increase their functionality to provide great value to their users. However, their use entails specific data protection risks due to the easiness of collecting great quantities of personal data and a potential lack of data protection safeguards.

These guidelines are intended to provide practical advice and instructions to the EU institutions on the processing of personal data in mobile applications to ensure that they comply with the data protection obligations set out in the Data Protection Regulation No 45/2001 applicable to the EU institutions.

While these Guidelines are in principle aimed at the EU institutions, anyone or any organisation interested in data protection and mobile applications might find them useful; the Regulation (EC) No. 45/2001 is similar in many respects to the Data Protection Directive (EC) 95/46 and to the new General Data Protection Regulation (Regulation (EU) 2016/679), both of them applicable to EU Member States, as well as in the EEA. Other countries that look to the EU data protection model can find them useful, too.

Summary of recommendations

These guidelines focus on specific aspects of data protection and mobile applications. These specific elements must be considered together with aspects applying to IT systems in general which are laid out in the 'Guidelines on the protection of personal data in IT governance and IT management of EU institutions'.

The mobile application must collect only those data that are strictly necessary to perform the lawful functionalities as identified and planned.

The requirements of valid consent apply to mobile applications. Users have to be given the option to change their wishes and revoke their decision at any time.

An essential element of consent is the information provided to the user. The type and accuracy of the information provided needs to be such as to put users in control of the data on their smart mobile device to protect their own privacy.

Some mobile applications use third party components or services that need to be used and managed accordingly to the Regulation.

The design and operation of the planned mobile application must follow an information security risk assessment.

Prior to investing in a mobile application, a data protection compliance analysis must be performed which could also lead the EU institution not to use a mobile application to support a certain task but rather use alternative solutions.

Actively involving the Data Protection Officer, and where relevant the Data Protection Coordinators or Contacts, early in the process of design of any new mobile application, will allow them to offer advice, suggest improvements and generally help the EU institution to ensure compliance with the Regulation.

1. Introduction

1.1. The Guidelines

1 When individuals use a mobile application developed by an EU institution, body or agency ('EU institution'), the EU institution is responsible for ensuring compliance with the data protection principles, in particular with Regulation 45/2001[1] ('the Regulation') in order to guarantee the rights to privacy and to the protection of the personal data of those individuals.

2 As the independent supervisory authority competent for the processing of personal data by the EU institutions, the European Data Protection Supervisor (EDPS) may among other tasks issue Guidelines on specific issues related to the processing of personal data[2]. The present Guidelines are the result of a process where the EU institutions have been consulted.

3 These guidelines provide practical advice and instruction to the EU institutions as controllers on the application of the Regulation to the development and the operation of mobile applications developed by the EU institutions. They are aimed at DPOs and DPCs within each EU institution, as well as IT and IT security staff, mobile applications business owners and other administrative services concerned with the design or operation of mobile applications.

4 While the purpose of these guidelines is to make it easier for EU institutions to fulfill their obligations, they do not take away any of the responsibility of the EU institutions applying them. The measures recommended in these guidelines are not intended to be exhaustive or exclusive. They are flexible enough to allow the EU institutions to start the expected process on accountability, and to be future oriented by considering expected legislative changes. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. Their effectiveness will need to be justified in writing.

1.2. Technical background

5 Mobile applications are software applications running on smart devices, in particular mobile ones like smartphones and tablets. Most of them are designed for wide-ranging and targeted interaction with web resources. They may also process location data[3] and other contextual information collected by many sensors[4] found in any smart device. Mobile applications are also able to exchange information via many network interfaces[5] with other connected devices.

[1] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[2] In the exercise of the powers conferred under Articles 41(2) and 46(d) of the Regulation.

[3] Through e.g. GPS signals and Wi-Fi spots positions.

[4] Sensors providing, e.g., movement (direction, speed and acceleration), video and audio capture, proximity detection.

[5] Such as Wi-Fi, Bluetooth, Near Field Communication techniques and protocols.

6 The operating systems (OS) running on these smart devices interact with those sensors and interfaces through software libraries and data structures (hereafter called APIs[6]). The mobile applications use the API to read information from sensors and exchange data with basic services.

7 The Article 29 Data Protection Working Party provided guidance on this topic in their '*Opinion 02/2013 on apps on smart devices'*[7]. The Opinion targets commercial mobile applications, and provides a comprehensive analysis with recommendations to all parties involved in the development and operation of mobile applications, including developers, OS and device manufacturers, and mobile applications stores. The general recommendations of this opinion are also valid for mobile applications provided by EU Institutions and are taken into account in the present Guidelines.

8 The EU institutions have started developing mobile applications for smart mobile devices to access their web services and provide new services.

9 This document focuses on the responsibilities of the EU institutions for the development and operation of mobile applications. As well as ensuring compliance, personal data protection is essential in order to obtain users' acceptance of the services, and thus foster the use of EU institutions' mobile applications.

2. Scope, methodology and structure of the Guidelines

2.1. Scope

10 These Guidelines provide advice on compliance with data protection rules in the context of the use of mobile applications developed and provided by the EU institutions. They address, in particular the development and operation of mobile applications to interact with the institutions' online information resources.

11 This document does not focus on:

- EU institutions' web services,
- the use of mobile devices by EU institutions' staff for professional purposes.

12 Those topics are dealt with in other EDPS thematic guidelines, such as the EDPS 'Guidelines on the protection of personal data processed through web services provided by EU institutions'[8] and the 'Guidelines on the protection of personal data in mobile devices used by European institutions'[9], respectively.

[6] Application Programming Interfaces

[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[8] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-07_Guidelines_Web_services_EN.pdf

[9] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-17_Mobile_devices_EN.pdf

2.2. Methodology

13 This document fits into action 8 of the EDPS Strategy 2015-2019[10], aiming to promote data protection culture, and at increasing the accountability towards data protection requirements in the institutions through specific guidance. In particular, the EDPS has identified a need for specific guidance in protecting personal data when the processing operations are 'technology intensive'.

14 The process leading to these Guidelines was designed as a structured open dialogue with the EU institutions. The core steps/elements of this process[11] are:

- a survey as a fact-finding exercise for collecting facts and reaching a better understanding of the EU institutions' position on the subject-matter;
- a workshop held on the topic and based on an orientation document preliminarily sent to the participants of the workshop, where the EDPS also presented the survey results;
- the review of best practices on mobile applications;
- the preliminary draft of the Guidelines sent to EU institutions for their feedback; and
- taking into account such feedback, the finalisation of the Guidelines.

2.3. Structure

15 This document is structured as follows:

- Section 1 and 2 introduce the Guidelines and describe scope, methodology and structure.
- Section 3 presents some specific risk associated to mobile applications.
- Section 4.1 outlines the general principles of data protection applied to the processing of personal data by mobile applications.
- Section 4.2 covers mobile applications specific security issues.

Text in italics and inside a box represents examples and clarifications to the content of the text above.

Rx: Recommendations come in boxes like this. Text with further advice and detail may precede or/and follow the box.

3. Specific risk factors linked to mobile applications

A survey (December 2013) commissioned by the UK's Information Commissioner's Office found that 62% of persons who have downloaded a mobile application are worried about the way mobile applications use personal data and that 49% of mobile applications users have decided not to download a mobile application due to privacy concerns.

[10] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/Strategy2015

[11] The process covered web services and mobile applications.

16 The use of mobile applications introduces specific issues to take into account when managing risks, which include[12]:

- More and more sensitive data are collected.

Mobile applications can collect large quantities of personal information from their many sensors, including location, biometric and other sensitive data. This information, processed together with the records of users' interaction with the web service, could also be used to build users' profiles and pose risks to their fundamental rights.

- Potential lack of data protection safeguards in view of the seamless interaction users expect from the smart mobile device.

It is more difficult, in the mobile context, to adequately inform users about the processing of their personal data than in the desktop environment (besides other factors, because of a smaller display size).

- Lack of information about data protection and security features of a mobile application.

Users are not adequately informed about the use of encrypted communications by the mobile application, whereas in many browsers the use of encryption (https) is usually visually displayed though icons, specific colour background etc.

- Lack of control over the underlying software layers: Device and operating system (OS) manufacturers provide the software layer interacting with the hardware (including sensors) and the APIs enabling the processing of the smart device data by the mobile applications. These components define the granularity of the mobile application developers' control over personal data processing and the configuration capabilities of services provided through the mobile application.

Some mobile OSs do not offer the capability of defining in sufficient precision what personal data a mobile application may use. Since, at least for commercial mobile applications, they very often process categories of data that are not necessary for the specific purpose of the mobile application, this limitation heavily reduces users' control over their personal data and puts into question the validity of their consent, unless the developer of the EU institution's mobile application mitigates this problem by designing such features at the mobile application level.

- Security measures strongly depend on the OS and the security services it provides. In general, smartphones and tablets' standard environments still offer lower security than traditional computers.

Unlike the applications running on desktop computers, mobile applications operate in changing environments usually not under control of the EU institution. They may use insecure third party services or even compromised, malicious access points or 'jailbroken', 'rooted' devices out of the control of the vendor.

- Use of external contractors who may have a poor data protection culture and practices: Current commercial mobile applications do not always provide adequate

[12] These considerations are made at the time of drafting these guidelines and may change in time.

safeguards to protect personal data. They may lack transparency and information to data subjects, along with specific privacy policies. In addition, they may not obtain free, specific, unambiguous and informed consent. They may disregard data protection principles such as purpose specification and limitation or data minimisation. Security measures could also be inadequate.

4. Obligations, recommendations and best practices

4.1. General principles for personal data processed by mobile applications

R1: Assess whether the mobile application processes personal data and which.

17 Personal data are processed when the mobile application interacts with a web service, or even when it just interacts with the smart device[13].

Examples of such interactions are providing contact details to subscribe to a newsletter or location data to find the closest centre providing the services sought or registering contact details in the agenda or saving data downloaded from a web service on local storage.

18 The general principles, obligations and recommendations given in the EDPS '*Guidelines on the protection of personal data in IT governance and IT management of EU institutions*'[14] apply to the development and operation of mobile applications, too.

All processing operations done through a mobile application must be lawful and the information to users must be complete.

19 Some obligations of major concern for mobile applications, in the light of the specific risks outlined in section 3, are further developed as follows.

20 The EU institution should take decisions on the design and operation of the planned mobile application based on an information security risk assessment (see EDPS '*Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001*')[15].

21 The EU institution should analyse the compliance of its intended processing before implementing the mobile application during the feasibility check, business case design or an equivalent early definition stage of the project. The compliance analysis must be open with respect to its outcome: it could also lead the EU institution to not use a mobile application to support a certain task but rather to choose an alternative solution. It is important to involve the DPO as early as possible to provide knowledgeable advice on data protection matters.

[13] Even if a mobile application processes personal data only on the device, the obligations of Article 5(3) of Directive 2002/58/EC (ePrivacy) still apply.

[14] In consultation when the present document was published.

[15] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf

4.1.1. Necessity and proportionality, purpose specification and limitation

R2: The mobile application must collect only those data that are strictly necessary to perform the lawful functionalities as originally identified and planned.

22 What the mobile application will do with the user's personal data needs to be clearly communicated to users before the installation of the mobile application.

E.g. through the mobile application description provided at the mobile application store or in an EU institution website page about the mobile application.

23 No processing for further incompatible purposes must be performed by the mobile application. Where the EU institution's internal rules provide for a change of purpose, this needs to be clearly communicated to the user before it becomes effective.

24 The mobile application must not communicate personal data to the EU institution or a third party unless this transfer is necessary for the purpose of the mobile application. Transfers should clearly be indicated in the information about the mobile application.

4.1.2. Managing consent

For a detailed analysis of the considerations to take into account in light of Regulation 45/2001 and Article 5(3) of the ePrivacy Directive[16] *and the recommendations to be followed in relation to the consent and information to users please see the EDPS 'Guidelines on the protection of personal data processed through web services provided by EU institutions'*[17] *and the Article 29 'Opinion 02/2013 on apps on smart devices'*[18].

R3: Adequately inform users and obtain their consent before installing any application on user's smart mobile device.

25 All requirements of valid consent apply to mobile applications. Users have to be given the option to change their wishes and revoke their decision at any time.

26 Consent needs to be collected before any reading or storing of information from/onto the smart mobile device is done. All essential elements of valid consent should be present at that time. That also means obtaining valid consent before installing the mobile application.

E.g. through a setup page inside the mobile application.

27 An essential element of consent is the information provided to the user. The type and accuracy of the information provided needs to be such as to put users in control of the data on their smart mobile device to protect their own privacy.

28 In particular the consent should be:

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.
[17] See footnote 8.
[18] See footnote 7

- Specific: The information provided to the user should highlight the type of data processed through the mobile applications, along with any related purposes.
- Expressed through an active choice: The procedure and tools used to obtain consent should allow users to express their wishes, with no margin of doubt about what their decision is. As such, those procedures and tools need to make sure that users actively confirm that they have been informed clearly and comprehensively about the way that their data will be processed, and that they fully consent to this.
- Freely given. Users should be given the opportunity to make a real choice, e.g. without being put under pressure or presented with a 'take it or leave it' approach.

29 Mobile applications must provide the users with:

- Real choices on personal data processing: The mobile application must ask for granular consent for every category of personal data it processes and every relevant use. If the OS does not allow a granular choice, the mobile application itself must implement this. In this case, the mobile application must clearly inform the user before the installation that, despite the OS settings, the user will have the opportunity of choosing what category of personal data to consent to through adequate functionalities directly provided by the mobile application;
- Functionalities to revoke their consent: The mobile application must feature functionalities to revoke users' consent for each category of personal data processed and each relevant use. The mobile application must also provide functionalities to delete users' personal data where appropriate.

4.1.3. Providing information to users in an effective way

R4: Provide appropriate information to the users so that they can take informed decisions.

30 The size of the smart mobile device screen and the seamless interaction mobile users expect to have with their device should not prevent users from being provided with the information they are entitled to under the Regulation.

31 The mobile application should therefore feature:

- A layered notice, where the initial notice to the user contains the essential information[19] and further information is progressively available through subsequent links. The information should be easily accessible and highly visible.
- Contextual real-time information can be provided through icons and images to show when certain categories of personal data (e.g. location or biometrics) are processed or certain measures are being implemented (e.g. security measures

[19] More information on the minimum information required and information to users in general can be found in the EDPS '*Guidelines on European institutions and bodies' accountability for the protection of personal data processed through IT systems*' (see footnote 14).

like the use of encryption). Video and audio could also be used to inform and raise users' awareness.

4.1.4. Providing mobile applications and choice of the supported hardware and OSs

R5: Evaluate the privacy capacities of target OSs and hardware.

32 When planning to deliver a mobile application and deciding for which hardware and operating systems (specifically which version) it shall be available, the EU institution needs to perform an assessment taking into account the nature of the personal data processed and the specific risks of any processing operations performed through mobile applications in smart mobile devices. The assessment also needs to take into account the targeted OSs' data protection and security features and practices.

If the mobile application is planned to process health data, and the OS does not allow enough granularity of choice for the user to decide what services/information the mobile application has access to, the EU institution might decide not to deliver a mobile application for that OS.

4.1.5. Mobile application distribution and mobile application stores obligations

R6: Evaluate the data protection impact of using a mobile application store to distribute a mobile application.

33 Mobile applications are usually distributed via mobile application stores, which are often owned by the same market operators as those providing the OSs and the mobile devices.

34 The EU institution should take into account that these mobile application stores are third party services (see section 4.1.6), controllers of their own for the personal data they manage and subject to all relevant obligations. The EU institution must give mobile application users all necessary information about controllers' respective responsibilities before they install the mobile application[20].

35 If the EU institution decides to distribute mobile applications through its own means, the following obligations need to be considered:

- enable the provision of the necessary information to prospective users before the mobile application installation, in order to obtain informed consent (see also consent related issues above in this section);
- ensure integrity of mobile applications against malicious or accidental unauthorised changes aimed at installing malicious mobile applications;
- make mobile applications new functionalities and bug fixes rapidly available for download;
- the distribution is reliable, which involves checking the security of the means chosen and providing users with information on the checks performed.

[20] See sections 4.1.2 and 4.1.3.

4.1.6. Third party components or services in mobile applications

R7: Assess the data processing features of a third party component or of a third party service before integrating it into a mobile application.

Where third party components or services are used within the EU institution's mobile applications, the EU institution should assess how these tools collect and process personal data, including transfers from the mobile applications to servers operated by a third party. The EU institution should also take account of general considerations regarding the use of third parties in IT systems management, as explained in the EDPS 'Guidelines on European institutions and bodies' accountability for the protection of personal data processed through IT systems'[21].

Third party components include software development kits (SDKs), programming frameworks and libraries, either for generally making the development of mobile applications easier, or for specific purposes, such as displaying photos or maps, or communicating via social media.

Third party services may receive data from the mobile application and process it, e.g. to perform analytics on the usage of the mobile application or they may host specific content for the mobile application on central servers.

36 If third party servers operated outside the EU and the EEA are used, it is imperative to take into account the applicable rules regarding data transfers to third countries.

37 For detailed technical and practical guidance on transfers of personal data to third countries and international organisations by EU institutions, see also the EDPS Position Paper of 14 July 2014 '*on the transfer of personal data to third countries and international organisations by EU institutions and bodies*'[22].

4.2. Security

4.2.1. Security of processing

R8: Apply appropriate information security risk management to the development, distribution and operation of mobile applications.

38 One fundamental principle of data protection is security. Through an information security risks management process the EU institution needs to identify the relevant risks to the personal data processed through the mobile applications provided and then to take appropriate organisational and technical measures to protect that personal data. Detailed advice on information on information security risk management can be found in the EDPS '*Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001*'[23].

39 The security measures produced by the information security risk management process will constitute part of the non-functional requirements of the mobile application being

[21] See footnote 14

[22] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf

[23] See footnote 9.

considered. This process needs to be performed as soon as possible to guarantee the better security with the lowest cost: data protection, or security, by design.

40 It is then very important to implement these security measures with the right technology. For that reason, it is important to stay abreast of new developments in threats and vulnerabilities, and their most effective countermeasures. This can be done in various ways including:

- having security consultancy for the development of mobile applications;
- using information sources like the OWASP community[24] where the most common current threats and vulnerabilities for all kind of applications are described, together with possible countermeasures; or
- using guidelines from ENISA[25].

41 If external contractors are used, the EU institution needs to ensure that the processor has put in place the appropriate technical and organisational security measures that the processor applies to protect personal data.

4.2.2. Data breaches

R9: Adopt internal procedures for the handling of security and data breaches that foresee in particular the notification of the occurrence of such events by the controller to the DPO.

A data breach in one of its mobile applications should be reported internally according to the EU institution's policy on the handling of security and data breaches. The DPO should assess and document the breach and the measures taken in reaction for future assessment and verification and consider whether it is appropriate to inform the EDPS. The EDPS response to such data breaches will obviously depend on a number of factors including the seriousness of the breach, the type and volume of data involved, the numbers of users affected, the location of the recipients, etc.

42 Data breach notification to the users is highly recommended. Accountability requires that the users should be adequately and promptly informed on incidents concerning their data, on how to protect themselves and on the incident follow-up insofar as it relates to possible risks for them.

4.2.3. Secure development, operation and testing

R10: The EU institution should have documented secure development policies and processes for mobile applications, including operation and security testing procedures following best practices.

43 An integrated security testing approach plays an essential role in the development phase (with security static code analysis and dynamic approaches such as penetration testing).

[24] '*OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.*' - https://www.owasp.org/index.php/Main_Page

[25] European Union Agency for Network and Information Security: http://www.enisa.europa.eu/

44 Adequate and up-to-date training on mobile application secure development, operation and security testing should be provided to the IT staff involved.

45 The EU institution can benefit from existing relevant best practices and guidelines[26].

46 No 'production' data[27] must be used for testing in the implementation or acceptance phases. Where the simple production of random test data sets is insufficient in a specific context, more sophisticated techniques for creating synthetic[28] data need to be used, which mimic the structure of real world data but do not contain any personal data.

The generation of synthetic data is often based on an analysis of the structure and other specific features of anonymised data sets from the real world. Synthetic data should enable the creation of realistic datasets without compromising the privacy of the users.

4.2.4. Vulnerability management

R11: Adopt and implement a vulnerability management process appropriate to the development and distribution of mobile applications.

47 The EU institution needs to regularly test the mobile applications developed for vulnerabilities that may endanger the personal data processed through them but also the smart mobile devices of the users installing the mobile applications.

48 The EU institution must have a process in place to react to reports on security issues of its mobile applications, whether directly from users or via the media or other channels.

49 In addition, the EU institution needs to monitor and address the vulnerabilities present in the components used to develop its own mobile applications, e.g. libraries, frameworks, etc. The manageability of those components, e.g. the frequency of upgrades, need to be considered when choosing a particular component or other.

50 The vulnerability management process shall ensure that updated mobile applications are provided as early as possible and that users are alerted to the need to install the updates.

51 The OSs and the physical mobile devices will reach their end-of-life and will no longer be supported by their vendors. It is important for the EUIs to consider which OSs versions are supported by their mobile applications.

4.2.5. Protection of personal data in transit and at rest

52 When personal data are sent over public or not-trusted networks such as the Internet they need to be protected against the risks raised by those networks.

[26] E.g. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines or https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

[27] Data actually processed by the mobile application during its normal operations.

[28] Synthetic data are data generated to meet specific needs like protecting the confidentiality of personal data.

The EU institution needs to take into account threats such as ‘man in the middle’ attacks[29]*, or unsecure Wi-Fi hot-spots with no or weak encryption.*

53 Mobile applications should use encryption to protect these communications through an adequate encryption layer (like TLS[30]) configured properly, together with a secure management of the relevant cryptographic keys[31].

E.g. never ’hard code’ or store cryptographic keys in the device where an attacker could recover them, such as plain text data files or property files.

54 Personal data also needs to be protected when stored in the smart mobile device, e.g. through effective encryption of the personal data.

[29] https://www.owasp.org/index.php/Man-in-the-middle_attack

[30] Transport Layer Security (TLS): ‘*The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.*’

[31] See for example RFC 7525 ‘Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)’ (https://tools.ietf.org/html/rfc7525) or the reports by ENISA ‘on cryptographic protocols’ (https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols) or on ‘Algorithms, key size and parameters (2014)’ (https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014)

Annex I. Glossary

Accountability
Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.

Consent
In data protection terminology, consent refers to a freely given, specific and informed indication of the wishes of a data subject, by which he/she agrees to personal data relating to him/her being processed. Consent is an important element in data protection legislation, as it is one of the conditions that can legitimise processing of personal data. If it is relied upon, the data subject must unambiguously have given his/ her consent to a specific processing operation, of which he/she shall have been properly informed. The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect.

Data controller
Under the Regulation, the data controller is the institution or body that determines the purposes and means of the processing of personal data. The data controller is also responsible for the security measures protecting the data.

Data minimization
The principle of ’data minimization’ means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.

Data security
According to Article 22 of the Regulation, the data controller shall implement appropriate technical and organisational measures to ensure an appropriate level of security in relation to the risks represented by the processing and the nature of the personal data to be protected.

Mobile application
A computer program designed to run on a smart mobile device such as smartphones or tablet computers. Although they are capable of processing and storing information locally, most mobile applications are connected to web services.

Mobile application store
A digital distribution platform for mobile applications. They are typically online stores, where users can browse through these different mobile application categories, view information about each mobile application, and acquire the mobile application. Most important mobile application stores are controlled by their owner and prospective mobile applications need to pass an approval process.

Personal data
According to Article 2 (a) of the Regulation: ‘Any information relating to an identified or identifiable natural person, referred to as "data subject" - an identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity’.

Processing (of personal data)
According to Article 2 (b) of the Regulation, processing of personal data refers to ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.’

Right of information
Everyone has the right to know that their personal data are processed and for which purpose. The right to be informed is essential because it determines the exercise of other rights. The right of information refers to the information that shall be provided to a data subject whether or not the data have been obtained from the data subject.

Annex II. References

Article 29 Data Protection Working Party *Opinion 02/2013 on apps on smart devices*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

EDPS *Guidelines on the protection of personal data processed through web services provided by EU institutions*:

EDPS *Guidelines on the protection of personal data in mobile devices used by European institutions*: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-17_Mobile_devices_EN.pdf

EDPS Strategy 2015-2019: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/Strategy2015

EDPS *Guidelines on the protection of personal data in IT governance and IT management of EU institutions*:

EDPS *Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001*: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf

EDPS Position Paper of 14 July 2014 *on the transfer of personal data to third countries and international organisations by EU institutions and bodies*: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf

OWASP webpage: https://www.owasp.org/index.php/Main_Page. '*OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.*'

European Union Agency for Network and Information Security: http://www.enisa.europa.eu/

ENISA *Smartphone Secure Development Guidelines*: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines

Projects/OWASP *Mobile Security Project - Top Ten Mobile Risks*: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

RFC 7525 *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*: https://tools.ietf.org/html/rfc7525

ENISA *Study on cryptographic protocols*: https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

ENISA *Algorithms, key size and parameters report 2014*: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014