Developing GDPR compliant applications, Part 1: A developer's guide to the GDPR

Understand how the GDPR impacts you

Dave Whitelegg

May 25, 2018

This article is the first part of a three part series on developing applications that are compliant with the European Union's General Data Protection Regulation (GDPR). It summarizes the GDPR and explains how the privacy regulation impacts and applies to developing and supporting applications that are intended to be used by European Union citizens.

Introduction

The General Data Protection Regulation (GDPR) was created by the European Commission and Council to strengthen and unify Europe's data protection law, replacing the 1995 European Data Protection Directive. Although the GDPR is a European Union (EU) regulation, it applies to any organizations outside of Europe that handle the personal data of EU citizens. This includes the development of applications that are intended to process the personal information of EU citizens. Therefore, organizations that provide web applications, mobile apps, or traditional desktop applications that can indirectly process EU citizen's personal data or allow EU citizens sign in are subject to the GDPR's privacy obligations. Organizations face the prospect of powerful sanctions should applications fail to comply with the GDPR.

This article, the first in a three-part series, summarizes the GDPR and explains how the privacy regulation impacts and applies to developing and supporting applications that are intended to be used by European Union citizens. Part 2 explores how to integrate privacy risk evaluation and mitigation within the software development lifecycle, and Part 3 provides practical application development techniques that can alleviate an application's privacy risk.

Consequences of GDPR non-compliance

The GDPR grants each EU country's data privacy regulator, known as a supervisory authority, with corrective powers and financial sanctions to ensure organizations comply with each EU citizen's right to privacy. Sanctions for non-compliance include fines of up to €20 million or 4 percent of the global turnover of the organization, and giving EU citizens the legal right to claim compensation for damages through class action lawsuits. The GDPR also mandates the disclosure of personal data breaches within 72 hours, which can also result in significant reputational damages and the loss of consumer trust due to adverse media attention.

The objectives and overview of the GDPR

The 1995 EU Data Protection Directive (95/46/EC) relied upon each EU national government's interpretation of requirements, but the GDPR applies exactly as it is worded, to any organization in the world that processes the personal information of EU citizens. The regulation itself consists of 99 Articles and 173 Recitals. The Articles are the obligations (requirements), while the Recitals support and explain how the Articles should be considered and applied.

You can see the GDPR Articles and Recitals in full, however, they can be challenging for non-legal and non-data privacy professionals to understand.

Throughout this series, I refer to the GDPR Articles and Recitals by their GDPR reference number, and the Article paragraph number follows within brackets.

GDPR key terms and definitions

To ensure applications are developed to comply with the GDPR and to mitigate privacy risk, you should gain a good understanding of the right to privacy, the GDPR requirements, and key data privacy terms. This knowledge can assist you in handling privacy enquiries by development project sponsors, Data Protection Officers, and the users of the application.

The fundamental right to privacy

Privacy is a fundamental human right recognized by the United Nations, within international treaties and within over 150 national constitutions. The right to privacy in the broadest sense is the right of an individual to be left alone from unwanted intrusion and observation by other people. This includes the non-disclosure of private facts about the individual to third parties or publicly without their permission.

In the digital frame, an individual's right to privacy is often misunderstood or neglected; perhaps this is due to the mass proliferation of personal data sharing on social media, or the regular reporting of large personal data breaches by the media. However, the fundamental human right to privacy is still as valid in the digital context as it is in the physical world.

Common digital privacy intrusions by organizations include:

- Not obtaining consent from individuals before collecting and processing their personal information (in other words, their private facts)
- Not clearly informing individuals about how their personal information will be used and shared with other parties
- Collecting excessive personal information from individuals without reason
- Not providing individuals with visibility and control over their personal information
- Not allowing individuals to exercise their privacy rights

- Not sufficiently protecting personal information (for example, providing poor security)
- Not informing individuals when their personal information is compromised

The GDPR has been devised to address these digital privacy shortcomings, ensuring organizations fully comply with an individual's right to digital privacy, through the stipulation of a descriptive set of privacy obligations for organizations to follow.

Data subject

A data subject is the individual to whom personal data relates.

Personal data

Personal data is defined as any information that can be used to identify a person, including indirectly through a nickname or reference number.

Personal data examples include an individual's:

- Name
- Application user ID
- Email address (even those not including a name)
- Account number
- Forum and online handles
- Any other identifier that can be looked up in a database to identify an individual
- Biometric data, including genetic data
- Location data

Location data

Location data is regarded as personal data under the GDPR, and it is any data that can be used to identify where an individual lives, works, or plays. Developers should be aware that cookie strings, IP addresses, geo tagging data, and mobile device identifiers are all regarded as personal data, given such data can be used to locate and identify an individual.

Potential hidden personal data within applications

Developers should recognize that fields of information that by themselves are not classified as personal data can become personal data when they are combined with other fields within a record. Developers should review the potential usage of any free text fields by the application, where there is any reasonable likelihood that text fields could hold personal data (for example, via user input), such text fields should be regarded as personal data.

Article 4 (1) '*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of t hat natural person;*

Personal data that has been pseudonymised (in other words, key-coded methods like tokenization and encryption) still can considered as personal data, depending on how difficult it is to attribute the pseudonym back to identifying an individual. Refer to Part 3 of this series for further details about pseudonymization.

Where one or more fields within a record can identify an individual, the other fields within the same record that hold private facts about the identified individual is also regarded as personal data.

Personal data cannot be processed by applications without having a lawful basis to do so under Article 6 (1), which includes obtaining user consent.

Article 6(1) *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; refer to Article: 7, 8 & 9 and Recital: 32, 42, 43 & 171

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; refer to Article: 20

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Refer to Article: 13 & 21 and Recital: 113, 47 & 48

Special categories of personal data

Special categories of personal data are types of personal data that are considered to carry a more significant risk to an individual's rights and freedoms. As per Article 9 (1) special categories of personal data includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health, sex life, or sexual orientation
- Genetic data
- Biometric data

Special categories of personal data can only be processed on a lawful basis, as cited in Article 6 & 9. Obtaining explicit consent from the individual, as Article 9 (2a), is the most common method of achieving a lawful basis.

Where special categories of personal data are required to be processed, the data should be protected with the strongest of security measures, such as applying database encryption. Compromise of special categories of personal data is likely to result in the most significant enforcement measures by supervisory authorities.

Given the additional security overheads and increased risk with the usage of special categories of personal data, developer leads should always verify and challenge any proposed usage put forward by project sponsors, ensuring that there is a clear, lawful purpose for such data to be used by the application.

Data protection officer

Most organizations need to designate a suitable data protection professional in the role of a data protection officer (DPO). Article 39 states that the DPO role is to inform and advise the organization on its GDPR obligations and to monitor compliance with the GDPR, including within the application development and support processes. The DPO is also the primary point of contact for data subjects and supervisory authorities.

Personal data responsibility role definitions

Like the precursor EU Data Protection Directive, the GDPR defines two types of organizational personal data responsibility roles: a data controller and a processor. But unlike the directive, the GDPR places further responsibilities and liabilities on data processors and includes processor organizations that host applications used by other organizations. With each application developed and supported, you must clearly understand if your organization is in a position of a controller or a processor, as the responsibility of facilitating most of the GDPR individual privacy rights lies with controller organizations.

Controller

A controller is an organization responsible for determining the purposes and means for processing personal data. Where an organization develops applications for internal usage only, the organization is typically in the role of a controller.

GDPR Article 4 (7) '*controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;*

Processor

A processor is an organization that processes personal data as instructed by, or on behalf of, a controller. Where the development and deployment of applications is for resale and usage by other organizations, including the provision of application hosting, the application providing organization is typically in the role of a processor. Where providing applications for processor organizations, you should still consider developing and providing such applications with the necessary functionality to aid controller organizations in facilitating GDPR privacy rights through the application.

GDPR Article 4 (8) *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

Obtaining consent

The GDPR places emphasis on organizations obtaining the data subject's consent prior to accessing and handling their personal data. For applications, consent usually means obtaining each user's permission before completing an account sign up process, as this is typically the initial personal data collection made by the application. Consent requires the data subject to be clearly informed about how their personal data is processed and stored by the application, including any third-party access and data sharing, and then requesting and recording the user's permission.

GDPR Article 4 (11) requires consent to be obtained through a positive action by the data subject. This means that if the application provides a consent statement with a permission tick box, the tick box must be set to empty by default, so that it requires the user to take an action to check the agree consent tick box. This is considered gaining consent through a clear affirmative user action.

Article 4 (11)*'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

The application must track when user consent was obtained by date and, ideally, time. Recording consent allows the application to demonstrate evidence of user consent, which is required under Article 7 (1).

Article 7 (1)*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

The application must have a dedicated privacy consent statement that must be separate and not part of any other license or service agreements. The privacy statement must be written in a clear and concise manner and explain in detail how the user's personal data will be processed by the application. This is required by Article 7 (2).

Article 7 (2)*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

The data subject has the right to withdraw their consent at any time, as stipulated within Article 7 (3). For applications to comply, the application must provide users with a simple user consent withdrawal function. If consent withdrawal is enacted by the user, the application should process the full deletion of all instances of the user's account and personal data, including where such data is held on backup systems.

Article 7 (3) *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

Article 7 (4), supported by Recital (43), requires user consent to be freely given, which means data subjects should not be forced to sign up and give their consent to use the application as a precondition in receiving a service.

GDPR Article 7 (4)*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

Child consent

If the application is intended or has potential to be used by data subjects under the age of 16 years (children), consent must be obtained by a person holding parental responsibility for the child. This is a requirement of Article 8 (1 & 2). Therefore, reasonable efforts must be made to verify the individual providing parental consent is actually the parental figure for the child's account. An application solution to this requirement, along with age verification, is to request consent through an additional parental account that is linked to the child's account. The application can verify that the parental account's email address is active and different to the email address associated with the child's account. Such a verification process could be regarded as making reasonable efforts as opposed to providing an additional parental consent tick box during the child's account creation process.

Article 8 (1) *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

Article 8 (2)*The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology* .

GDPR privacy rights

Applications that process the personal information of EU citizens are in scope of a number of specific GDPR privacy rights. Developers need to ensure applications are developed and maintained with the appropriate measures and functionality to faciliate the following GDPR privacy rights to the users of the application:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subjected to automated decision making, including profiling

The right to be informed

Applications that process personal information must be completely transparent with users in how their personal data is processed. This should be facilitated to each application user through a privacy statement or privacy notice. A common mistake when writing a privacy statement is to use application development language and terms. The privacy statement must be written using common language terms so that it can be easily understood by individuals that are non-technical and not data privacy experts. To aid understanding, consider using graphical pictures and flowcharts within the privacy statement, to provide a visual representation of how the application processes their personal information.

If the application is intended to be used by children, then the privacy statement has to be written using wording that children can understand.

The privacy statement should describe the personal information collected and processed by the application. In addition, the statement should justify all use of personal data by the application by providing specific reasons for all data collection and data processing by the application. The privacy statement should also clearly describe any other third-party organization involvement with the application's processing of personal data, including any third party hosting (for example, data storage, including backups), any accessibility (for example, third-party remote support), and any transfer or sharing of data with other third-party organizations.

Article 12 (1)*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. Also see Recital 58 and Recital 59.*

The right of access

EU citizen application users have the right to access all of their personal data as held and processed by the application. The organization operating the application is the controller and the party responsible for facilitating this right to application users. To aid an organization's GDPR compliance, applications should be developed to facilitate a user's right of access by including a user function that returns all of the user's personal data, as held by the application.

Data subject access requests

The right of access also means application users are entitled to make a written request to be provided with either all, or specific parts, of their personal information, as held by the application and the controller organization. This process is known as a data subject access request. The GDPR requires data subject access requests to be provided free of charge and within a month of the request. Where an organization is a controller, they should provide contact details for application users to make data subject access requests and have a formal process to manage such requests in a timely manner.

Article 15 (1)*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.*

The right to rectification

Application users have the right to have their personal data corrected where it is inaccurately held or incomplete, as per Article 16. To aid controller compliance, applications should provide users with the functionality to edit their own personal data records. Every field of personal data should be editable in case of accidental input error, or should the personal data become outdated, for instance, when a user has a change in their residential address, or following a change in their marital status (for example, a new surname). Applications should regularly remind users to verify their personal data is accurate and complete.

The application should record all changes to personal data and provide a formal notification of all changes to the data subject. This can be achieved in most cases by an email notification. The communication of changes to personal data is required for Article 19 and is also a good security practise as users are quickly informed should another party illicitly change their personal data without their knowledge. Typically, after compromising an application user account, hackers change the account password, email address, and postal address to aid fraudulent and nefarious activity.

Article 16*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*

Article 19*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out*

The right to erasure

The right to erasure, commonly known as the "right to be forgotten," gives application users the right to instruct a controller to delete all of their personal information, including where their data is held on database backups and with processors. There are legal circumstances where the Article 17 right does not apply, so a criminal simply can't expect to have their criminal record deleted upon request. But generally, for most commercial orientated applications, the application should include a user function where a user can instruct the deletion of their account and all personal data held. The account erasure process should also include the deletion of all account and personal data held on backup systems. The application must also provide the user with a confirmation once all their personal data has been erased, which is required under Article 19.

Article 17*(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.*

Article 19*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out*

The right to restrict processing

EU citizens have the right to block the processing of their personal data under Article 18. Where this right is invoked by a data subject with a controller, it means the application is still allowed to hold a data subject's personal information, but it is not permitted for the personal information to be processed by the application. An application can facilitate this right by allowing the user's account to be set as inactive or dormant. The application user must be formally notified (i.e. by email) when facilitating this right by making their account inactive, this is required for Article 19.

Article 18 (1)*The data subject shall have the right to obtain from the controller restriction of processing*

Article 19*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out.*

The right to data portability

The right to data portability gives an application user the right to request to move or copy their personal data between different controller organizations. The data transfer must use an acceptable data format, and be perform securely. Data portability requests should be completed within one month and organizations are not allowed to charge a fee.

An application data export function can expedite data portability requests, as per Article 20, by exporting a data subject's personal data records from the application into a CSV formatted file. The CSV format is considered an open and universally accepted 'machine-readable' data format, which permits other controller organizations to automate the input of the data subject's personal data into their applications and systems without hindrance.

The transfer of personal data between controller organizations must be adequately secure, and must be encrypted where the personal data is transferred over non-trusted or public media and environments.

Article 20 (1) *The 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 controller to which the personal data have been provider. See Recital 68*

The right to object

EU application users have the right to object to their personal information being used for profiling, direct marketing, and for scientific or historical research, a right given under Article 21.

Objection to profiling

The GDPR defines profiling under Article 4 (4). In simple terms, it means using an individual's personal information and statistical data to build a profile about the type of person they are, how they behave, their health, their financial position, or where they are located. Where applications intend to perform user profiling, the activity should be made clear within the privacy statement, where user consent is obtained. The user should be given the option to object to profiling and disable the application's profiling processes, ideally within the user's account controls.

Article 4 (4)*Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

Objection to direct marketing

Applications that are capable of sending marketing messages to users, including by email, text message, social media posting, and postal mail, must initially obtain user consent to do so. Marketing consent should be provisioned through a dedicated opt-in, with a clear statement about the type of marketing messages expected to be sent by the application, the communication channels used, and a consent tick box. The consent tick box must be defaulted as not ticked when initially presented to the user. Applications should also provide users with the ability to opt-out of direct marketing messages at any point in time.

Article 21 (2)*Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*

Objection to scientific or historical research

If personal data processed by the application is intended to be used for research purposes, users should be given the ability to object to such usage under Article 21 (6), unless the research is in the public interest.

Article 21 (6)*Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

Refer to Article 12 and 89 and Recitals 156, 157, 158, 159, 160, 161, 162, and 163.

The right not to be subject to automated decision making including profiling

Article 22 requires users to be clearly informed and be given the ability to object, if the application analyzes or profiles their personal information, for purpose of gaining an insight into their behaviours and characteristics. This includes where an application makes automated decisions based on personal data analytics, including any effects it may have for the user and on their personal data. Such activity must only be performed if there is a legitimate requirement.

Article 22 (1)*The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*

Conclusion

To develop applications that are compliant with the GDPR, you need a working understanding of data privacy key terms and definitions. This helps you to better converse with data privacy subject matter experts in explaining issues and comprehending advice when developing privacy risk mitigation solutions, as part of an application's development and support.

You also need to be familiar with all the individual privacy rights afforded to application users by the GDPR. This helps ensure all application processes and user functionality are designed and coded to facilitate the applicable GDPR privacy rights to application users.