Developing GDPR compliant applications, Part 2: Application privacy by design

Dave Whitelegg

May 25, 2018

This article provides guidance for integrating privacy risk evaluation and mitigation within the software development lifecycle. It is part 2 in a series of articles about developing applications that are compliant with the European Union's General Data Protection Regulation (GDPR).

Introduction

An application's privacy risk considers the potential distress and harm caused to application users, should users lose control over their application-managed personal information. Organizations that directly provision applications to users are subject to their own privacy risk, which takes into account the controller organization's potential reputation damages and financial impact, should the application fail to provide EU citizen users with the privacy rights afforded by the General Data Protection Regulation (GDPR). Therefore, integrating an application privacy by design, also referred to as data protection by design by the GDPR, within the software development lifecycle is an essential practice to ensure an application's privacy risk is thoroughly understood and evaluated, and where deemed appropriate, mitigated to an acceptable level of risk.

This article is Part 2 in a series of articles that provides guidance for developing applications that are compliant with the European Union's General Data Protection Regulation. Part 1 summarizes the GDPR and Part 3 explores practical application development techniques that can alleviate an application's privacy risk.

GDPR data protection by design requirement

GDPR Article 25 states data protection by design applies to organizations that are in the role of a controller, this directly applies to internally developed applications for use by the developer's organization. Where applications are developed for use by external organizations, those organizations as a controller, will seek to understand and verify the application's privacy risk with the application's developers. Therefore a data protection by design development approach should be adopted regardless of whether an application is intended for internal use, or for use by other organizations that are in a controller role.

GDPR Article 25 (2) requires data protection by design by default. This means that all of the application's privacy settings must be set to protect a user's privacy when the application is provisioned to users.

Article 25 Data protection by design and by default*1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, that are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article. Supported by Recital 78*

An essential tool in developing applications with data protection by design is a data rotection Impact Assessment.

Application data protection impact assessment

An application data protection impact assessment (DPIA) helps developers to identify, analyse, and explain how an application impacts the privacy rights and freedoms of its users. A DPIA should be performed against applications intending to collect, maintain, and/or share personal information.

By embedding a DPIA early within the software development lifecycle, developers are able to mitigate unacceptable privacy risks and resolve GDPR user privacy rights compliance issues before the completion of the application's design. This ensures that the application is efficiently developed to minimize privacy risk, which benefits users, and the risk to data controller organizations provisioning the application.

DPIAs should also be performed retrospectively against applications that have been previously released and in production to assure their privacy risk is acceptable and to verify their compliance with the GDPR.

Application DPIA roles and responsibilities

The expected roles and responsibilities involved with an application DPIA include:

- The developer lead is responsible for managing the application's DPIA process. Where there is not a developer lead, the DPIA responsibility should fall to the application development project manager.
- A data protection officer (DPO) or a data privacy subject matter expert is required to consult and support the DPIA process, which is cited as a DPIA requirement in GDPR Article 35 (2). *Article 35 (2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*
- A DPO can be externally sourced should the developer organization not have a DPO role, or an individual with the sufficient data privacy expertise. A DPO is also required to sign off the completed DPIA.
- An information security professional or an application security specialist is required to consult and to verify application security best practises are adopted throughout the application's development.
- A risk manager is recommended to consult and advise on privacy risk management practises.
- The development project manager should be informed about DPIA outcomes and actions.
- Project sponsors and business directors are accountable for privacy risk; therefore, they must be briefed and provided with a copy of the completed DPIA and the application's privacy risk register.
- Where applications are developed for external processor organizations, expect such organizations to request a copy of the application DPIA and application implementation privacy guidance as part of their own DPIA process, GDPR obligations verification, and privacy risk management.

Performing a DPIA within the SDLC

The application's GDPR privacy rights obligations should be documented as requirements within the requirements analysis phase of the Software Development Lifecycle (SDLC). The DPIA should be performed within the design phase of the SDLC. Then, further privacy risk verification should be conducted throughout the latter phases of the SDLC, to assure the application's privacy requirements are all achieved, and the application design mitigates or eliminates privacy risks as intended.

The Application SDLC (Waterfall Model) phases include:

1. Requirements analysis (GDPR privacy rights obligations)
2. Design (DPIA)
3. Development (Deliver DPIA outcome actions and GDPR rights functionality)
4. Testing (DPIA outcomes, GDPR rights functionality, and application security testing)
5. Implementation (privacy implementation guidance)
6. Maintenance (DPIA re-review and updates)

The GDPR privacy rights obligations are explained in the first part of this guidance series. Identified privacy risks should be evaluated with a view to designing technical application solutions that minimize the privacy risk, such as using database encryption and pseudonymization, these technical solutions are discussed in the third part of this guidance series.

Application DPIA process

There are six phases to an application DPIA:

1. Identify the need for a DPIA
2. Describe personal data flow
3. Identify privacy risks
4. Determine and evaluate privacy solutions
5. Document DPIA outcomes and sign Off by the DPO
6. Implement DPIA privacy solutions within the development plan

Identify the need for a DPIA

GDPR Article 35 (1) requires a data protection impact assessment to be performed where *"new technologies"* are *"likely to result in a high risk"* to individuals. The supporting Recital 75 describes privacy risks that are typical of applications processing personal data, stating *"where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage"*.

The development of a new application can be regarded as a "new technology" under Article 35 (1). While the GDPR does not specifically define "high risk", where applications process personal data on mass, it is likely most supervisory authorities would consider such applications as having an inherent high risk to user privacy, especially where the application is internet facing. Therefore unless the application has no potential to process EU citizen's personal information, it is recommended to perform a DPIA on all developed applications to comply with GDPR Article 35 (1).

Article 35 (1)*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

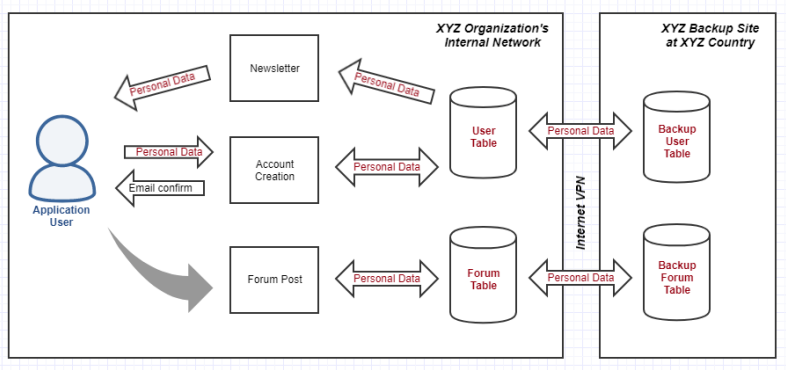
Article 35 (7)*Data protection impact assessment"The assessment shall contain at least:*
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Describe personal data flow

The application DPIA must be documented, which should start with a description of the application's general purpose, and a simple overview of the application's functions. Also record whether the application developing organization will be in a GDPR role of a controller (i.e. provisioning the application), processor (i.e. just hosting the application) or neither.

The next step is to determine and describe how personal information will be obtained, processed, stored, and moved out of the application. With assistance from the application architect, review and map the application's data flows and processes. Documenting with a data flow chart, allows the application's processes and personal data flows to be clearly described and understood, an example is shown in Figure 1.

Application dataflow example



In addition to the data flow diagram, further more comprehensive details about the application's personal data usage should be recorded. Review the application's design and explore the following aspects with the technical leads.

- Personal data collection
  - Personal data ingress:
    - The user account creation process
    - User data entry and data edit capabilities
    - Data transfers in i.e. data captured from third party sources
  - Personal data fields:
    - Document the specific field names and tables that hold personal data
    - Flag personal data fields that are considered direct or indirect personal identifiers i.e. name, email address, account number, location data
    - Flag personal data fields that are defined as 'Special Categories' of personal data under the GDPR i.e. biometric, health, race, political opinions, religion, genetic data
    - Flag personal data fields that can be used to locate or track an individual i.e. cookies, IP address, geometric data
    - Flag any non-designated personal data fields that potentially could hold personal data, such as text box fields i.e. a user freely typing in personal data into a description text box
  - Document the purpose of each personal data field: document the reason for the application obtaining and processing each personal data field identified

    - Document whether children will be able to use the application
- Personal data processing
    - Document how personal data will be used by the application
    - Detail any automatic changes to, or creation of personal data by the application: such as automated processing of personal data by the application, profiling processes, and any record keeping of user activity
    - Document where the application uses technology or processes that could be perceived as privacy intrusive: i.e. use of biometric, user location tracking and analysis of genetic data
- User access and interaction
    - Document the application user's interaction capabilities with their personal data:
        - User ability to view all of their personal data fields
        - User capability to edit and delete their personal data
    - Document any provided user account roles with privileged levels of access to personal data such as administrative, supervisor, support and reporting accounts that are able to access to multiple user personal data records. Detail the account role capabilities in accessing, changing and exporting personal data.
- Personal data storage
    - Record details of all databases\tables used by application to retrieve and store personal information
    - Describe where each database\tables is hosted (i.e. server/system) and where physically located: consider local hosting, third party\cloud hosting and backup systems
    - Detail any storage or use of personal data within monitoring and logging systems. i.e. local application server logs, application exports to syslog servers
- Personal data output
    - Document all personal data egress points: consider reports, email messaging, SMS, postal mail (printing), outward bulk data transfers and data extraction processes
    - Document any personal data sharing and accessibility
        - Sharing or access provided to third party organizations, other users within the application, connectivity with other applications or publically i.e. social media connectivity
        - Third party support i.e. remote technical support, system upgrades

A spreadsheet or a table is a useful method for documenting the application's technical personal data usage. Figure 2 depicts an example.

Application technical personal data usage

Field	Table	Database location	Data Ingress	Purpose	Data Subject Identifier?	Special Cat. Data?	Can Track Data Subject?	User Interaction	Accessible to other App Users?	Public Accessible?	Privacy Risk Notes
<full_name>	Users	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	Required personal identifier for the application user's profile	Yes	No	No	Edit, View	No	No	None
<app_user_id>	Users	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	Unique ID required to authenticate user account with application	Yes	No	No	View Only	No	No	Users will be able delete their account and all data, however, forum post may not be removed
<password>	Users	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	Required to authenticate the user's account with the application	No	No	No	Edit only	No	No	Password will be stored using a salted hash in the table
<email address>	Users	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	Required to notify the user of forum posts and comments, and to provide a monthly copy of the newsletter (if opted in), used for account recreation and for password resets	Yes	No	No	Edit, View	No	No	Notifications will be sent to the users, which will require a specific opt-in by the data subject, with opt-out enabled by default.
<forum handle>	Users	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	Required identify the data subject (user) on the forum	Yes	No	No	Edit, View	Yes	No	Forum handle can identify a data subject (directly or indirectly)
<religion>	Forum	Internal Data Centre, Backup in Cloud	Data subject requested input as part of the account creation process	The forum is religious, and the project sponsors seta a requirement for users to be optionally identify with their religion of choice on their forum account profile	No	Yes	No	Edit, View, Delete	Yes	No	Religion is not a mandatory field, users are asked to provide as part of account creation
<ip_address>	Forum, AppsLog	Internal Data Centre	Created and used by application security and logging processes	Application captures the users' device IP address for security purposes i.e. Tracking should the user's account be compromised by a third party	Yes	No	Yes	Field Not accessible	No	No	Confirmed this field will not used with any automated or profiling processed by the application

Identify privacy risks

The next step of the DPIA is to identify privacy risks by reviewing the personal data flow documentation. This review should be supported by the data protection officer or a data privacy subject matter expert. Also involve a risk manager or risk professional, to formally guide and document the privacy risk assessment.

There are three general groups of privacy risk to consider and document with an application DPIA:

- Application user (data subject) privacy risks
- Application privacy risks in facilitating the GDPR privacy rights to users
- Organization privacy risks as a controller or a processor

Application user privacy risks

When assessing the application's user privacy risk, consider the possible application intrusion scenarios to a user privacy rights and freedoms, with the likelihood of each privacy intrusion, and the potential impact on the user, such as personal distress and financial loss.

The following types of application privacy intrusions can negatively impact users and should be explored:

- Confidentiality: scenarios involving the unintentional or malicious compromise of personal data
- Integrity: scenarios leading to inaccurately held personal data
- Availability: scenarios that renders the application or personal data inaccessible to users

Describe each privacy risk scenario identified on a risk register. Each risk on the register should include an evaluated risk rating from factoring the privacy intrusion likelihood with the impact on user's privacy. An example of an application risk register is depicted in Figure 3.

Risk register

Risk ID	Risk Description	Likelihood	Impact	Risk Rating	Risk Owner
R01	The application's password reset process could be used to lock a user out of their account should their user account be compromised by a malicious third party	Low	Medium	Medium	Developer Lead
R02	The application process which permits the manual edit of user details by administrators could result in the inaccurate personal data, given the process uses an account lookup by a user's their full name instead of unique record identifier such as user ID or email. This means an administrator could update the wrong record details	Medium	Medium	Medium	Developer Lead
R03	A person under age of 16 (child) could put in a fake date of birth to create an account on the system	Low	Low	Low	Developer Lead

Application privacy risks in facilitating the GDPR privacy rights to users

There are a number of GDPR user privacy rights that impact applications, these rights are explained in the first part of this guidance series. With the support of the application architect, review the application's design documentation and assess how the application facilitates, or not, each of the applicable GDPR user privacy rights, these include:

- The right to be informed (Article 12)
- The right of access (Article 15)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- The right not to be subject to automated decision making including profiling (Article 22)

Document the application processes that adequately facilitates each of the GDPR privacy rights within the DPIA documentation. Where any of the applicable GDPR privacy rights are not adequately facilitated by the application, document these as privacy risks on the risk register.

Organization privacy risks

Organizations that are in the role of a controller or processor that fail to comply with the GDPR, are at risk of significant sanctions that include large fines by supervisory authorities, legal claims for damages by users, bans on processing personal data, and reputational damages. The organization's privacy risks should be assessed with the support of the DPO, and also recorded on the risk register.

Where the software developing organization intends to be in the role of a controller, namely provide the application directly to users, the following risks and their potential impact on the developing organization should be considered:

- Obtaining user consent and the accuracy of the privacy statement
- Avoiding the collection of excessive personal data
- Personal data breaches, unintentional or malicious data compromise, including on mass breaches of personal data
- Ensuring personal data remains up-to-date and accurate
- Failure to provision GDPR rights to application users, either within the application or directly by the organization as a controller
- The non-availability of the application or personal data i.e. system outages, backup recovery, malicious denial of service attacks

Determine and evaluate privacy solutions

The next stage is to assess each privacy risk recorded on the risk register with a view to accepting, reducing or eliminating each risk. The mitigation of privacy risk may be achieved by devising solutions and making changes to the application's design, implementing enhancements to the SDLC processes, or introducing procedures and controls at the controller organization. The application architect, technical lead, the Information Security Officer, and the DPO should all be involved in determining and evaluating privacy risk mitigating solutions.

The third part of this guidance series explains several common application privacy risk mitigation solutions, such as database encryption and pseudonymization.

Document DPIA outcomes and sign off by the DPO

The privacy risks on the risk register should be updated to reflect any risk mitigation changes made to the application's design, and include a residual risk rating, which is the assessed risk rating post the change. Ensure all privacy risk mitigation changes and solutions are incorporated within the application's design and project plan. The development project manager should be informed of the DPIA outcomes, to ensure risk mitigation actions are formally included within the development plan.

The completed DPIA documentation should include:

- An overview of the application, including its purpose and functions
- The GDPR responsibility of the application developing organization i.e. controller, processor or neither
- Personal data data flow diagram
- Technical personal data details e.g. spreadsheet
- Description of the application's GDPR user privacy rights processes
- Copy of the application's privacy statement
- Completed risk register that includes application user and organizational privacy risks
- DPO Sign off statement page

The DPO must review the completed DPIA documentation, if the DPIA is considered to be an accurate representation, and the privacy risk is deemed to be acceptable, and the application, and the organization where applicable as a controller or processor, fully compliant with the GDPR, the DPO should sign off the DPIA. Else the DPO should cite any issues and request further assessment.

The development project sponsors should be provided with a copy of the completed DPIA. As project sponsors are typically responsible for the overall privacy risk of the developed application, it is recommended they also should sign off the DPIA.

Implement DPIA privacy solutions within the development plan

The development project sponsors should be provided with a copy of the completed DPIA. As project sponsors are typically responsible for the overall privacy risk of the developed application, it is recommended they also should sign off the DPIA.

Application implementation guidance

Where applications are intended to be resold, hosted, or used by external controller organizations, developers should write and provide application implementation guidance, to assist controller organizations to provision the application to protect user privacy as designed, and by default. The implementation guidance should include concise step-by-step instructions on installing and configuring the application's privacy settings. The guidance should also recommend the security configuration of the application's supporting components, such as web servers, databases and the network environment.

To provide additional transparency and GDPR support to controller organizations, the implementation guidance should include a full explanation of all privacy related application functions and processes. The guidance should also detail where the controller organization is expected to be responsible for providing any user GDPR privacy rights that are not facilitated by the application, and for responsibilities on the controller organization to mitigate the application's privacy risk. This information will have already been obtained and included within the DPIA documentation.

Conclusion

GDPR Article 35 requires a data protection impact assessment (DPIA) to be performed where 'new technologies' are likely to result in a high risk to the privacy rights and freedoms of individuals. This requirement can be construed to apply to the development of any application that intends to process EU citizen personal data.

Completing a formal DPIA early within the software development lifecycle is an essential practice to efficiently develop applications that protects user privacy rights from the outset. Developers should seek support from data privacy subject matter experts, information security, and risk management professionals throughout the DPIA processes. In leveraging their expertise, developers are able to formally identify and evaluate both application user and organization privacy risks, and where risks are considered unacceptable, devise technical solutions to mitigate them within the application's design.