

Instructions

General Data Protection Regulation (GDPR) and ISO/IEC 29100 Privacy Framework to a Taxonomy of Privacy Requirements

Introduction

This guide follows the grounded theory and content analysis approaches to derive privacy requirements from written statements in the GDPR and ISO/IEC 29100 privacy framework. We create a range of questions to identify requirements from each statement. We will analyse 19 articles focusing on individual's rights and personal data processing in the GDPR and all of the contents in the ISO/IEC29100 privacy framework. The requirements will then be grouped into relevant categories. They will be finally refined to a taxonomy of privacy requirements. The taxonomy will be useful for software developers to understand complex legal statements in terms of implementable requirements. It also sets out a number of compliance regulations which the bodies handling the processing of personal data must meet.

Materials

This section lists the materials required in the extraction process.

Inputs

- The official Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
Articles 6-7, 12-22, 25, 29-30, 32-34.
(Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>)
- ISO/IEC 29100:2011 (First edition: 2011-12-15)

Process

- Form of privacy requirements identification.

Output

- A set of privacy requirements.

Steps

1. Privacy Requirements Identification

Goal: This step aims to extract requirements from written statements in the GDPR and privacy framework. We will use a set of questions to identify relevant components of the statements for constructing a privacy requirement.

Steps

a. Identify action

For each statement, we identify action by asking “*Which action should be provided based on this statement?*”. Some examples of the action verbs used in the collected statements are: ALLOW, ARCHIVE, COLLECT, ERASE, IMPLEMENT, INFORM, MAINTAIN, NOTIFY, OBTAIN, PRESENT, PROTECT, PROVIDE, REQUEST, SHOW, STORE, TRANSMIT and USE.

b. Determine involved/affected parties

After acquiring the action, it is necessary to indicate the object of that action by asking “*Who is involved/affected by that statement?*”. Please note that the objects are optional.

c. Consider the target result

This specifies the expected result that can be achieved to serve user privacy and rights by asking “*What should be achieved based on the action of that statement?*”.

d. Structure into a privacy requirement pattern

The derived privacy requirement is codified in the format of action verb, followed by object and objective complement.

Please note that steps a-c can be done in any order. For each step, the result is recorded into a form of privacy requirements identification and classification for reliability test and further discussion.

Example

Article 13 - Paragraph 1 - Point (a) states "... the controller shall, at the time when personal data are obtained, *provide the data subject the identity and the contact details of the controller and*, where applicable, of *the controller's representative*".

Follow the steps:

a. Identify action

=> *provide*

From this statement, we identify 'PROVIDE' as the action that the controller shall act.

b. Determine involved/affected parties

=> *the data subject*

Then, we determine the object responding to 'to whom the identity and contact details of the controller or the controller's representative should be provided', and that is the data subject.

c. Consider the target result

=> *the identity and the contact details of the controller and the controller's representative*

After that we consider what should be provided by the controller, and that was 'the identity of and the contact details of the controller or the controller's representative'.

d. Structure into a privacy requirement pattern

All three components formulate a privacy requirement as '*PROVIDE the data subject the identity and contact details of a controller/controller's representative*'.

Remark: If a coder considers that a statement is not related to the processing of personal data, he/she can mark as not to derive.

The outputs from this step will be taken into a reliability assessment before passing to the classification step.

2. Privacy Requirements Classification

Goal: This step aims to classify the privacy requirements obtained from the previous step into one of the following privacy goal categories based on their relevance. These goals are acquired from the seven GDPR principles.

Steps

- a. Set the achievements of each privacy goal (Perform only one time)

Our privacy goals are expected to gather all the privacy requirements that aim to achieve similar compliance based on the GDPR principles. Therefore, we will describe and elaborate the expected achievements of each goal in this step.

- b. Consider the expected outcome that a requirement achieves

In this step, we will classify each privacy requirement into the relevant goal based on the expected achievements.


In the form, please select the drop-down list to assign each requirement into a privacy goal category.

Privacy Goal Categories

1. Lawfulness, fairness and transparency

This privacy goal ensures that personal data will be processed lawfully, fairly and in a transparent manner. The processing of personal data must be necessary. The data subjects must be informed of their individual rights. The controller must treat data subjects equally (i.e. every data subject shall have access to the same right). The controller must provide relevant information related to the processing of personal data to the data subjects. The information also includes contact details of responsible persons who control the processing. The data subjects must be notified when they are likely to be in risk from personal data exposures.

2. Purpose limitation



This privacy goal asserts that personal data must be collected and used for the specified and legitimate purpose(s). It should not be further used in any processing apart from the initial purposes. The controller must obtain consent from the data subjects for processing their personal data for specific purposes. The data subjects shall be provided options to/not to allow processing their personal data based on specific purposes.

3. Data minimisation

The privacy goal endorses the collection process of personal data. The controllers shall collect and store only the personal data that is required for the processing as specified within the purposes.

4. Accuracy

This privacy goal ensures that the processing of personal data is accurate and up-to-date. The data subjects have the rights to ask for erasure or rectification if their personal data is processed inaccurately of the specified purpose(s). There should be mechanisms to ensure the accuracy and quality of processing. In case that personal data are updated (i.e. removed or modified), all the relevant stakeholders must be notified to ensure the accurate use and processing of personal data.

5. Storage limitation

This privacy goal addresses the process of storing personal data. The data subjects must be informed of the duration used to store their data. The personal data shall be disposed when it is no longer necessary for the specified purposes. However, it may be kept further if required by laws or regulations with safeguarding measures.

6. Integrity and confidentiality

This privacy goal aims to ensure that the personal data and the processing of personal data are protected with appropriate controls and security mechanisms. The security mechanisms must comply with security and data protection standards.

7. Accountability

The goal privacy asserts that the controllers who are the main responsible actors for collecting the personal data and specifying the purpose(s) of processing shall demonstrate that the processes comply with the six goals mentioned above. Any processing of personal data must be available for compliance audit. In addition, the controllers shall adopt concrete and practical measures for the processing of personal data. The controllers have to ensure that the processors and third parties who process personal data as instructed by the controllers have equivalent technical measures to affirm reliable personal data transfers between organisations. In case of data breach, the controllers must notify a supervisory authority and relevant stakeholders with details.

Example

Article 13 - Paragraph 1 - Point (a)

'PROVIDE the data subject the identity and contact details of a controller/controller's representative'

Follow the steps:

- a. Set the achievements of each privacy goal
=> see Privacy Goal Categories section
- b. Consider the expected outcome that a requirement achieves
=> We need to classify the requirement above into one of the above categories. To do so, we consider the expected outcome that this requirement achieves. It aims to provide the contact of responsible person to users, thus it can be classified into the lawfulness, fairness and transparency goal category.

3. Privacy Requirements Refinement

Goal: This step aims to identify and manage those similar and duplicate requirements as well as format the structure and wording of the requirements.

Steps

- a. Manage duplications
- b. Observe inconsistencies
- c. Format structure and wording

Example

A statement in GDPR, "... the controller shall ... provide the data subjects with ... the existence of the right to withdraw consent at any time ..." derives a requirement:

'PROVIDE the existence of the right to withdraw consent at any time'

A statement in ISO/IEC 29100, "... allow a PII principal to withdraw consent easily and free of charge ...", derives a requirement:

'ALLOW a PII principal to withdraw consent easily and free of charge'

Follow the steps:

- a. Manage duplications

Both of these requirements are classified into the lawfulness, fairness and transparency category since they are related to the data subjects' right to give consent for their personal data processing. They can be considered the same requirement since both of them are concerned with the right to withdraw consent.

- b. Observe inconsistencies with other requirements
- c. Format structure and wording

Hence, we merge them into a single requirement: *'ALLOW the data subjects to withdraw consent at any time without cost'*.