A Taxonomy of Privacy Requirements

The taxonomy consists of 71 privacy requirements in 7 goal categories. Each requirement can belong to several categories.

Category 1: User Participation (9 Requirements)

The user participation category consists of a set of requirements for the controllers to provide the data subjects with the functionalities to invoke their individual rights relating to their personal data. The data subjects must be able to access, review, rectify, erase and verify the validity and completeness of their personal data. The personal data must be obtained and reused for different purposes across different services. The controllers shall allow the data subjects to object to and restrict the processing of their personal data. The data subjects must be able to withdraw consent or lodge a complaint to a supervisory authority.

R1 ALLOW the data subjects to access and review their personal data

R2 ALLOW the data subjects to lodge a complaint with a supervisory authority

R3 ALLOW the data subjects to object to the processing of their personal data

R4 ALLOW the data subjects to restrict the processing of their personal data

R5 ALLOW the data subjects to verify the validity and correctness of their personal data

R6 ALLOW the data subjects to withdraw consent

R34 ALLOW the data subjects to obtain and reuse their personal data for their own purposes across different services

R44 ALLOW the data subjects to erase their personal data

R45 ALLOW the data subjects to rectify their personal data

Category 2: Notice (32 Requirements)

The notice category consists of two sub-categories: data subjects and relevant parties. This category has a set of requirements for the data subjects to be informed and/or notified of relevant information and individual rights related to the processing of personal data. The information includes privacy policies, procedures, practices and logic of the processing of personal data. The data subjects must be informed of the purposes of collection and processing of their personal data. The controllers must provide the contact details of responsible persons who control the processing. The data subjects must be notified when they are likely to be at risk from personal data exposures. In addition, the controllers must communicate any relevant information relating to personal data processing to intended stakeholders.

Subcategory 2.1: Data Subjects

R9 INFORM the data subjects about the transfer of their personal data to a third country or an international organisation

R10 INFORM the data subjects prior to the elimination of their restriction of processing

R11 INFORM the data subjects the individual rights relating to the processing of personal data

R12 INFORM the data subjects the reason(s) for not taking action on their request and the possibility of lodging a complaint

R14 NOTIFY the data subjects if their personal data will be processing on other legal basis

R15 NOTIFY the data subjects the data breach which is likely to result in high risk

R16 NOTIFY the data subjects when major changes in the personal data handling procedures occur

R18 PROVIDE the data subjects an option not to be subject to a decision solely based on automated processing

R19 PROVIDE the data subjects an option to choose whether or not to provide their personal data

R20 PROVIDE the data subjects with the contact details of a data protection officer (DPO)

R21 PROVIDE the data subjects the existence and relevant information of automated decision-making including profiling

R22 PROVIDE the data subjects with the identity and contact details of a controller/controller's representative

R23 PROVIDE the data subjects the information about the source of personal data if they are not directly provided by himself/herself

R24 PROVIDE the data subjects the information of action taken on their request of individual's rights

R25 PROVIDE the data subjects the information of granting or withholding consent

R26 PROVIDE the data subjects the information relating to the policies, procedures, practices and logic of the processing of personal data

R27 PROVIDE the data subjects the recipients/categories of recipients of their personal data

R28 PROVIDE the data subjects the sufficient explanation for the need to process sensitive personal data

R29 PROVIDE the data subjects the consequences of not providing personal data based on the statutory or contractual requirement

R30 PROVIDE the data subjects the information relating to the processing of personal data with standardised icons

R37 PROVIDE the data subjects the additional information when further processing is required for a purpose other than the consent obtained

R38 PROVIDE the data subjects the purpose(s) of the collection of personal data

R39 PROVIDE the data subjects the purpose(s) of the processing of personal data

R42 PROVIDE the data subjects the categories of personal data concerned

R54 PROVIDE the data subjects the data retention and disposal requirements

R55 PROVIDE the data subjects the period/criteria used to store their data

Subcategory 2.2: Relevant Parties

R17 SHOW the relevant stakeholders the consent given by the data subjects to process their personal data

R50 INFORM the recipients of personal data any rectification or erasure of personal data or restriction of processing

R66 NOTIFY a supervisory authority the data breach

R67 NOTIFY relevant privacy stakeholders about a data breach

R68 PROVIDE the data processor a channel to notify a data breach

R71 PROVIDE a supervisory authority the information about a data breach

Category 3: User Desirability (9 Requirements)

The user desirability category consists of three sub-categories: consent, choice and preferences. This category asserts that the controllers must show a consent form to and obtain consent from the data subjects. The controllers must provide the data subjects with an option to provide their data, allow the processing or subject to a decision based on automated processing. The processing should be implemented based on user preferences expressed in their consent.

Subcategory 3.1: Consent

R6 ALLOW the data subjects to withdraw consent

R8 IMPLEMENT the data subject's preferences as expressed in his/her consent

R25 PROVIDE the data subjects the information of granting or withholding consent

R32 SHOW the data subjects a consent form in an intelligible and easily accessible form using clear and plain language

R35 OBTAIN the opt-in consent for the processing of personal data for specific purposes

R47 ERASE the personal data when a consent is withdrawn

Subcategory 3.2: Choice

R18 PROVIDE the data subjects an option not to be subject to a decision solely based on automated processing

R19 PROVIDE the data subjects an option to choose whether or not to provide their personal data

R36 PRESENT the data subjects an option whether or not to allow the processing of personal data

Subcategory 3.3: Preference

R8 IMPLEMENT the data subject's preferences as expressed in his/her consent

Category 4: Data Processing (16 Requirements)

The data processing category addresses the processes of personal data handling from the controllers' side. The processes, which are the sub-categories in this category, include collection, use, storage, erasure, transfer and record. The controllers must handle personal data as necessary for specific purposes. The processors who process personal data must also follow the instructions from the controllers. The personal data processing activities must be recorded.

Subcategory 4.1: Collection

R41 COLLECT the personal data as necessary for specific purposes

R49 IMPLEMENT the personal data collection procedures to ensure with accuracy and quality

R59 IMPLEMENT appropriate technical and organisational measures to ensure the personal data is collected, processed, and stored as necessary

Subcategory 4.2: Use

R40 USE the personal data as necessary for specific purposes specified by the controller

R59 IMPLEMENT appropriate technical and organisational measures to ensure the personal data is collected, processed, and stored as necessary

Subcategory 4.3: Storage

R43 STORE the personal data as necessary for specific purposes

R51 ARCHIVE the personal data when required by laws

R59 IMPLEMENT appropriate technical and organisational measures to ensure the personal data is collected, processed, and stored as necessary

Subcategory 4.4: Erasure

R7 ERASE the personal data when it has been unlawfully processed

R46 ERASE the personal data when the data subjects object to the processing

R47 ERASE the personal data when a consent is withdrawn

R52 ERASE the personal data when it is no longer necessary for the specified purpose(s)

R53 ERASE the personal data when the purpose for the processing has expired

Subcategory 4.5: Transfer

R9 INFORM the data subjects about the transfer of their personal data to a third country or an international organisation

R33 TRANSMIT the personal data to another controller when requested by the data subjects

Subcategory 4.6: Record

R13 MAINTAIN a record of personal data processing activities

R69 DOCUMENT the details of data breach to a supervisory authority for compliance verification

R70 DOCUMENT the categories of personal data collected

Category 5: Breach (6 Requirements)

The breach category ensures that the controllers must be prepared to handle personal data breach. The relevant information about the data breach must be recorded and communicated to data subjects and relevant stakeholders.

R15 NOTIFY the data subjects the data breach which is likely to result in high risk

R66 NOTIFY a supervisory authority the data breach

R67 NOTIFY relevant privacy stakeholders about a data breach

R68 PROVIDE the data processor a channel to notify a data breach

R69 DOCUMENT the details of data breach to a supervisory authority for compliance verification

R71 PROVIDE a supervisory authority the information about a data breach

Category 6: Complaint/Request (5 Requirements)

The complaint/request category addresses complaint and request management. User complaints and requests about their individual rights and the processing of their personal data must be processed. The actions regarding the complaints and requests must be informed. The controllers must request for relevant information to confirm the identity of data subjects when the request has been made.

R2 ALLOW the data subjects to lodge a complaint with a supervisory authority

R12 INFORM the data subjects the reason(s) for not taking action on their request and the possibility of lodging a complaint

R24 PROVIDE the data subjects the information of action taken on their request of individual's rights

R31 REQUEST the data subjects the additional information necessary to confirm their identity when making a request relating to the processing of personal data

R33 TRANSMIT the personal data to another controller when requested by the data subjects

Category 7: Security (13 Requirements)

The security category ensures that personal data and its processing are safeguarded with confidentiality, integrity and availability. The personal data must be protected with appropriate controls and security mechanisms. The security mechanisms must comply with security and data protection standards. The personal data must be accessed and used by the authorised stakeholders. The controllers must ensure the correctness and completeness of personal data.

R48 IMPLEMENT control mechanisms to regularly check the accuracy and quality of collected and stored personal data

R49 IMPLEMENT the personal data collection procedures to ensure with accuracy and quality

R56 ALLOW the authorised stakeholders to access personal data as instructed by a controller

R57 IMPLEMENT a process for regularly assessing the effectiveness of the measures to ensure the security of processing

R58 IMPLEMENT appropriate technical and organisational measures to comply with data protection principles

R59 IMPLEMENT appropriate technical and organisational measures to ensure the personal data is collected, processed, and stored as necessary

R60 IMPLEMENT appropriate technical and organisational measures to protect personal data

R61 IMPLEMENT the ability to ensure the ongoing security principles and resilience of processing systems and services

R62 IMPLEMENT the ability to restore availability and access to personal data in timely manner after physical or technical incidents

R63 PROTECT the personal data from unauthorised access and processing

R64 IMPLEMENT a function to limit the linkability of personal data collected

R65 IMPLEMENT a function to comply with local requirements and cross-border transfers

R69 DOCUMENT the details of data breach to a supervisory authority for compliance verification