giz

THE DEVELOPMENT OF A DATA PROCESSING SYSTEM UNDER THE GDPR

Personal data is any information that, alone or in combination with other pieces of information, can lead to the identification of a natural person or be attributed to that person. It ranges from direct identifiers such as names, email addresses, to indirect or remote identifiers such as one's farm size or just the exact time of a website visit.

The development of a data processing system may not necessarily involve the processing of personal data. However, since these systems, such as apps, websites, internet platforms, software, cameras etc., are meant for processing personal data, there are some preconditions to be fulfilled. The systems must fulfill the necessity requirement and take into account the privacy by design and by default obligations. This document offers practical guidance on compliance with such requirements.

1. THE NECESSITY REQUIREMENT

A data processing tool must be designed to process personal data only when its intended goal cannot be attained without such data. For example, if anonymous information would serve the purpose, then no personal data should be processed. Examples of anonymous information include:

- age range instead of one's exact age or date of birth (1-5 years; 6-10 years; 11-15 years etc.);
- income range instead of one's exact income (1000-3000 EUR; 4000-6000 EUR; 7000-10000 EUR etc.) ;
- farm size range (1-3 acres; 4-6 acre; 7-10 acres; more than 10 acres);
- range of number of persons living in a household (1-3 persons; 4-6 persons; 7-10 persons etc.);
- preferring general terms to specific terms (e.g. to determine one's employment status, you may indicate: employed, self-employed, and unemployed, instead of a particular occupation);
- using larger geographical groupings instead of smaller ones (e.g. identifying one's region, instead of his village or neighborhood).

Also, questions should require “yes” or “no” answers, and where specific information is required, options can be listed for the person to choose. Where the individual’s response does not fall among the suggested answers, he/she should be required to choose “other”, without providing space for the person to disclose any detailed information that may uniquely identify him/her.

Any other identifiers (figures/places/etc.) should be diluted, to render identification impossible.

This category of information is considered anonymous because it cannot lead to the identification of a natural person, neither can it be attributed to that person. In case personal data such as (but not limited to) names, IP addresses, email addresses etc. are to be processed, then the tool must comply with the following privacy by design and by default requirements in paragraphs 2 and 3 below.

2. DATA PROTECTION BY DESIGN AND BY DEFAULT

The system should be designed in a manner that takes into account the data protection principles (especially lawfulness, data minimization, transparency, integrity and confidentiality, accuracy, storage limitation and accountability), as well as the numerous rights of the data subject, as explained in paragraph 3 below. Additionally, it must be ensured that:

- by default, the system's privacy features are turned on and the users must take no action to protect their personal data;
- privacy features are embedded in the design of the system to ensure that the system can never run without such features;
- protection throughout the lifecycle is considered.

3. DATA PROTECTION PRINCIPLES AND THE NECESSARY RIGHTS

a. Lawfulness of data processing

By virtue of this principle, personal data should only be processed if one (the data controller) is permitted by law to do so, and one of the generally permissible ways is to process such data with the consent of the data subject. Consent is one of the most appropriate legal bases for processing personal data with digital tools. However, for such consent to be valid, it must fulfill the following requirements:

- by default, all features that require consent must be turned off, unless the user actively turns them on;

- the consent must be for a specific purpose (not for a bundle of purposes) and where consent is required for more than one purpose, it must be separately sought for each of them, e.g. two separate checkboxes are respectively required for the use of non-essential cookies and the sharing of personal data with a third party;

- the data subject must be well informed about the processing activity, including his right to withdraw consent (see subparagraph e. *"Transparency", below*);

- the consent must be unambiguous (through an affirmative action e.g. ticking a checkbox, but not opting out a pre-ticked checkbox. Silence would not qualify as acceptance);

- whenever special categories of personal data (such as biometric data, data relating to health, sexual orientation or sexual life, religious or philosophical believes etc.) are processed, the consent must be explicit. This equally applies to profiling and automated decision-making. That is, the system must require authentication (e.g. by SMS) or an electronic signature, to dismiss any doubts as to whether consent was given or not. Explicit consent is equally required to access one's bank account or process financial information during online payments;

- consent must be easily revocable and refusing to consent must not lead to the denial of service or be detrimental in any way to the user, or else such consent would not be considered to have been freely given. For example, the data subject should be capable of refusing consent to the use of non-essential cookies and still have access to the website. If the consent is a precondition for accessing the website, such consent would be invalid.

i. Essential cookies (not subject to consent)

According to the WP29 (now European Data Protection Board), the following cookies, considered essential, can be used without the data subject's consent under certain conditions, if they are not used for additional purposes:

- user input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases;

- authentication cookies, used for authenticated services, for the duration of a session;

- user centric security cookies, used to detect authentication abuses, for a limited persistent duration (few hours);

- multimedia content player session cookies, such as flash player cookies, for the duration of a session;

- load balancing session cookies, for the duration of session;

- UI customization persistent cookies, for the duration of a session (or slightly more); and

- third party social plug-in content sharing cookies, for logged-in members of a social network.

Despite being excluded from consent, these non-essential cookies remain personal data, and one still needs a legal basis to use them. Processing carried out for the controller's legitimate interest would be the most suitable legal basis, which must be indicated in the privacy notice.

ii. Non-essential cookies (subject to consent)

According to the WP29, non-essential cookies require consent. These include:

- social plug-in tracking cookies;

- third party advertising cookies; and

- first party analytics.

Where consent for several cookies is required, the user should be presented a "**Reject All**" option, especially when the "Accept All" option is equally presented.

Where possible, the system must be capable of preserving evidence that consent was actually granted, and such evidence must continue to be preserved for as long as the consent-based processing takes place (in line with the accountability principle).

b. **Data Minimization**

According to this GDPR principle, where the aim of the processing can be achieved with little amounts or less intrusive personal data, then large amounts or more intrusive

data should not be used. Thus, the minimization must be both **qualitative and quantitative**. Here are some practical examples.

- A surveillance camera is meant to take only pictures and videos of those who enter a given premises or place. So therefore, it should be impossible for it to carryout voice recording, as it would be considered disproportionate.

- In relation to an online platform, it must be ensured that there is no space for the data subject to enter unnecessary information. A recruitment portal should not require applicants to upload their photos, since only skills, qualifications and experience would be evaluated, and not appearance.

- Also, one's age (e.g., 15 years) should be preferred to one's date of birth, because the date of birth is more intrusive than age, although they both qualify as personal data (while age range does not). In a given classroom, for instance, a given student's date of birth would uniquely identify him/her, while many students of the class may be of the same age.

- To authenticate through a mobile phone number, only the last three digits must be disclosed to users instead of the entire mobile phone number. This does not only apply to phone numbers, but to bank accounts or similar data, as masking most digits of such data prevents disclosures to persons other than the data subject. This applies to email addresses too, where only the first three letters should be shown.

- Requiring one's field of occupation in a broad sense would be more appropriate than requiring one to specify his/her profession.

Data minimization is usually achieved by combining personal data with anonymous data, rather than using only personal data.

c. Storage limitation and the right to erasure

It is not allowed to process or store personal data longer than necessary.
The system must ensure that after the objective of the processing has been achieved, the data must be automatically erased by the following technical ways:

- facilitating the programming of automatic deletion for a certain period;

- in the case of an online platform, it must be ensured that the data of users who have not accessed their account for a certain period are automatically deleted after notifying such users; and

- the deletion must be permanent.

Alongside this principle is the right to erasure, which empowers data subjects to get their data deleted at any time. The system must therefore make it possible for data subjects to easily delete their accounts including all the personal data therein. A system that does not provide for these possibilities is not suitable.

d. **Data accuracy and the right to rectification**

To implement this principle and right, the system must:

- process only factually correct data, including correct time, correct location, and ensure that it is impossible to falsify this information;

- allow the data subject to correct inaccurate or outdated data; and

- allow applicants to update their previously submitted information (for example, job application documents).

The processing of inaccurate data may have a detrimental effect on the data subject, as he or she may either be denied a service or falsely implicated in situations that do not concern him or her, because of such inaccurate information (e.g. inaccurate location data showing one's presence in a crime scene).

e. **Transparency**

The system must provide information on all aspects of the processing to the data subject.

- The user needs to know what data are collected (processed) and how, why and by whom they are collected, and how to contact the controller. Where they are stored, for how long, who has access to them, whether he/she is obliged to provide such data and the consequences of not providing them.

- He/she should also know whether there are any data transfers outside the EU and what measures are in place to ensure the security of these data.

- The rights of the data subject must equally be communicated to him/her, including the rights to erasure, rectification, objection to processing, withdrawal of consent, complaint to the competent supervisory authority, etc.).

- The information can be provided through layered privacy notices and symbols. The Data HelpDesk would readily help you write a GDPR-compliant privacy notice.

- The information must be explicit enough, in simple language, so that even people without technical knowledge can understand it.

- Information about anything that would surprise the user must be brought to the user's attention first.

- Any data processing without the user's knowledge is not allowed.

f. **Integrity and confidentiality**

The system shall process data in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by implementing appropriate technical and organizational measures, such as:

- (end-to-end) encryption during data transmission; if the server is not in the EU: encryption of data at rest;

- pseudonymizing personal data;

- securing remote database access (e.g. via HTTPS or other suitable protocols);

- protecting user accounts with a secure password (minimum length, specialcharacters, etc.) or two-factor authentication;

- improving or updating of security features; and

- certifying the system in accordance with STANDARDS, if a certain standard is available or necessary.

These measures must take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the associated risks.

g. **Data portability**

If technically feasible, the data processing system shall allow the data subject to easily transfer his/her data to another service provider or other processing systems.

h. The rights to restrict or object to processing

The system should also be designed in such a way that makes it possible to suspend the processing of personal data, without necessarily deleting such data. This can be achieved through the deactivation of one's profile, either by the controller or by the data subject himself. This is because, the data subject has the right to restrict processing or object to such processing under certain circumstances, and this, after clarification or the fulfillment of certain requirements, may lead to the resumption of the processing activity, thus the reinstatement of the deactivated profile. During this deactivation or suspension of processing, the personal data should be well preserved as they are, but invisible and inaccessible.

i. Other considerations

It should be noted that we, data controllers, are required to engage only reliable processors to process personal data on our behalf. In this regard, you should seek advice on how to choose and contractually engage hosting and maintenance service providers of the digital tool. You would equally be orientated on how to submit a record of processing activities. These requirements are applicable when the said tool will be used by the GIZ, and not a local partner.