giz

ANNEX 2.

THE CREATION OF A DATA PROCESSING SYSTEM UNDER THE GDPR

The development of a data protection system does not usually involve the processing of personal data. However, since such systems, such as Apps, websites, internet platforms, software, cameras etc., are meant for processing personal data, there are some preconditions to be fulfilled. The following principles and rights should be strictly followed by the contractor when developing a data protection system.

1. Data protection by design and by default

-The system should be designed in a manner that takes into account universally recognized 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 explained below (**2.**);

- By default, the system's privacy features must be turned on and the user must take no action to protect their personal data;
- Privacy features must be embedded in the design of the system to ensure that the system can never run without such features;
- Protection throughout the lifecycle must be considered.

2. General Data protection principles and the necessary Rights

a. Lawfulness of data processing:

Processing of personal data requires that there is a legal permission to do so or that the data subject has consented thereto. For such consent to be valid, it must fulfill the following requirements:

- by default, all features that require consent must as a standard be turned off, unless the user explicitly turns them on;
- the consent must be for a specific purpose (not for a bundle of two or more purposes) and where consent is required for two purposes, consent must be separately sought for each of them, e.g. providing two different check-boxes, rather than just one for both purposes;
- the data subject must be well informed about the processing activity, including his right to withdraw consent (please see para. 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);
- whenever special categories of personal data (such as health data, data relating to sexual orientation or sexual life, religious or philosophical believes etc.) are used, the consent must be explicit. This equally applies to profiling and automated decision-making. That is, the system must permit authentication (e.g. by SMS) or an electronic signature, to dismiss any doubts as to whether consent was given or not;

- consent must be easily revocable and refusing to consent must not lead to the denial of the service or any other detriment, or else such consent would not be considered to have been freely given;
- 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.

  However, non-essential cookies, such as social plug-in tracking cookies, third party advertising cookies, and first party analytics **do require consent**.

- For cookies requiring consent, a user should be presented a "**Reject All**" option.

- Where possible, the system must be capable of preserving evidence that consent was actually granted, and such evidence must be preserved as long as the consent-based processing takes place.

b. **Data minimisation**:

The data processing system must be designed to process only data that are necessary for the processing purpose.

- For example, if the surveillance camera system is meant to take only pictures and videos, then in this case voice recording must be impossible.
- In relation to an online platform, it must be ensured that there is no space for the data subject to enter unnecessary information. Apps must not collect additional information that is not necessary.
- This principle also requires the use of aggregates rather than detailed information. If possible, one should use age (e.g. 20 years) instead of date of birth.
- 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.

According to this principle, where the aim of the processing can be achieved with little amounts of personal data, then large amounts of data must not be used. Where the goal can be reasonably attained without the processing of personal data, the processing of such data would be inappropriate.

c. **Storage limitation and the right to erasure**:

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:

- it must be possible to program automatic deletion for a certain period;
- in the case of an online platform, it must be ensured that data of users who have not accessed their account for a certain period are automatically deleted after notifying the users;
- the deletion here must be permanent.

Alongside this principle is the right to erasure, which empowers data subjects to get their data deleted at any time.

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 ensures that it is impossible to enter incorrect objective information (such as time and location).
- Allow the data subject to correct incorrect inaccurate or outdated data.
- An online application system that does not allow applicants to update their previous submitted applications is not in compliance with standards. This also applies to similar situations.

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 presence in a crime scene).

e. **Transparency:**

The system must be clear and must inform the data subject of all aspects of the processing, including how the data subject can exercise his or her rights (e.g. the rights to erasure, rectification, objection to processing, withdrawal of consent, complaint to the competent supervisory authority, etc.).

- The user needs to know what data are collected (processed) and how, why and by whom are they collected, and how to contact the controller. Where are they stored, for how long, who has access to them and whether he is obliged to provide such data and what are the consequences of not providing them.
- He should also know if 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, including his right to withdraw consent (where applicable) and that to complain with a supervisory authority or seek sue before a competent court.
- The information can be provided through layered privacy notices and symbols. **The Data HelpDesk would happily help you write a GDPR-compliant privacy notice.**
- The information must be explicit enough, with 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 inadmissible.

f. **Integrity and confidentiality**:

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

- (End-to-end) encryption during data transmission;
- Especially if the bidder and/or the server is not in the EU: encryption of data at rest;
- Secure remote database access (e.g. via HTTPS or other suitable protocols);
- Protection of user accounts by a secure password (minimum length, special characters, etc.) or two-factor authentication;
- Improvement or update of security features by the client; and
- Certification of the software in accordance with STANDARDS, if a certain standard is available or necessary.

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 programmed in such a way that makes it possible to temporarily 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 or 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, unless after reactivation.