PRIVACY POLICY

Document version:	v 2.0
Version Date:	25.5.2018.
Created by:	Marko Špoljarić
Approved by:	Zdenko Ćorić
Date of approval	6.2.2026
Confidentiality level:	PUBLIC
Distribution List:	ALL

Record changes to a document

Date	Version	Created by	Description of changes
25.5.2018	1.0	Goran Polonji	Basic draft of the document
2.2.2026.	2.0	Marko Špoljarić	Harmonization of the document with the requirements of the ISO 27701 standard

Contents

Intended use

The purpose of this document is to define the general policy and rules applicable to the protection of all personal data relating to natural persons (hereinafter: data subjects) obtained by Utilis d.o.o. (hereinafter: Utilis) in the course of its regular business. The policy also prescribes responsibilities for the processes of managing records of personal data processing activities, the register of data subject requests, the register of personal data breaches (incidents) and the register of consents.

The policy is based on the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - General Data Protection Regulation (hereinafter: GDPR).

Scope

This policy applies throughout the Utilis organization to all processing in which personal data of individuals (data subjects) is used. It is harmonized with all acts that in their individual parts touch on the protection of personal data or data in general (Information System Security Policy, Regulations and Procedures).

Definitions

Overview of terms and their meaning:

GDPR Regulation - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.

Data subject - Any individual (natural person) from whom we collect and process personal data.

Personal data processor – the role of a contractual partner (third party) of Utilis who is entrusted with the processing (or part of the processing) of personal data on behalf of the personal data controller.

Processing of personal data – means any action or set of operations performed on personal data, whether by automatic means or not, such as collecting, recording, organizing, storing, adapting or modifying, retrieving, viewing, using, disclosing by transmission, publishing or otherwise making available, collating or combining, blocking, deleting or destroying, and performing logical, mathematical and other operations with such data.

Personal data - All data about a data subject (natural person) that can be used to uniquely identify the same natural persons/individuals – data subjects. Personal data is all data used by

Utilis in its business that relates to an identified or identifiable individual (hereinafter referred to as the "data subject"). An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Consent of the data subject – a freely given and explicit expression of the data subject's will by which he expresses his consent to the processing of his personal data for certain purposes.

Personal Data Controller – is the role of the responsible person of Utilis who determines the purpose and manner of processing personal data collected from data subjects.

Principles

Security of personal information - Utilis protects personal information from unauthorized access, use, or disclosure. The collected personal data is stored in electronic form to which appropriate technical, organizational and procedural measures have been applied to prevent unauthorized access to personal data that is not accessible to other users and to ensure that it is used in accordance with our Policy and applicable regulations. In doing so, Utilis uses good practices related to information security, which are prescribed by other internal acts, starting with the Information System Security Policy.

Purpose of collection – Personal data will be collected primarily to ensure the provision of the requested service. Any processing that is carried out on personal data will clearly have a defined purpose of processing. Personal data may be processed only when there is a clearly defined and documented legal basis or a basis based on a contractual relationship, while all other processing of personal data is permitted only with the clear documented consent of their owner or representative.

Necessity of collection - When collecting and processing personal data, it is mandatory to apply the principle according to which only those data that are actually necessary for the processing in question may be collected. Any collection of redundant data is prohibited.

Storage limitation – Personal data must be kept in a form that allows the identification of the data subject only for as long as necessary for the purposes for which the personal data is processed. The exception is personal data that will be processed exclusively for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes that must be adequately secured in accordance with the GDPR.

Accuracy and timeliness of data – Utilis will ensure all necessary measures to ensure the accuracy and timeliness of personal data used in the processing.

Access to personal data – access to the personal data of data subjects may only be granted to those persons who need it to perform the service defined by the purpose of processing. The controller may, if necessary, engage a processor with whom he will conclude a contract and

bind him with security measures regarding the handling of personal data. The treatment of processors is also prescribed by the Ordinance on the Management of Third Apartments. The Processor, if he is not sure who is allowed to give access to personal data, will consult with the Personal Data Controller. Utilis may conclude international agreements that include the transfer of personal data to third countries or international organizations to the extent that such agreements do not affect the GDPR Regulation or any other provisions of Union law and that include an adequate level of protection of the fundamental rights of data subjects.

Informing data subjects - Before collecting personal data, data subjects must be provided with clear information about the reason for collection, the type of processing in which the information will be used, the data retention period and any third parties who will access the information. If Utilis collects personal data through the Utilis website, more detailed information for visitors to the Utilis website, who leave their personal data, will be prescribed by the privacy policy that will be posted on the Utilis website.

Processing of children's personal data - If data is collected from children, it is necessary to establish special mechanisms to ensure that children are old enough to understand the consequences of providing information. Any collection and processing of information by minors must be approached with special care, and must be guided by the highest ethical principles. For children under 16 years of age, parental consent must be obtained.

Special categories of personal data – Special attention should be paid to special categories of personal data with regard to safeguards. This data includes, for example, data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data relating to health, or data concerning an individual's sex life or sexual orientation. For the processing of this data, it is mandatory to carry out an assessment of the impact on the privacy of the data subject.

"**Privacy by design**" - When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data in order to fulfil their task, manufacturers of products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and to ensure, taking into account the state of the art, that controllers and processors processing may comply with their data protection obligations.

Responsibilities

The rules defined by this policy must be followed by **all employees of Utilis**, as well as **third parties** who have access to the personal data of data subjects as part of their cooperation with Utilis. Confidentiality and confidentiality statements and contracts ensuring compliance with the requirements of the GDPR regulation will be signed with third parties identified as processors of personal data.

The Personal Data Controller (TOOP) **is responsible for the establishment and maintenance of the personal data management system and the coordination of all activities related to personal data management** . He reports directly to the management of Utilis. The personal data controller is responsible in particular for:

- informing and advising the controller or processor and employees who process personal data about their obligations under the GDPR Regulation,
- monitoring compliance with the Regulation and internal policies and other regulations related to the protection of personal data,
- establishment and maintenance of a register of personal data processing,
- assigning responsibility for the protection of personal data to workers and third parties involved in the collection and processing of personal data,
- raising awareness and education in the field of personal data protection,
- embedding privacy protection in business processes and information systems,
- Embedding privacy protection in audit processes.
- advising on the implementation of data protection impact assessments (risk assessment or DPIA),
- cooperation with supervisory authorities;
- Monitoring the risk management process in personal data processing (PP) DPIA),
- reporting to the Management Board of Utilis on the effectiveness of the personal information management system.

The personal data controller is appointed by the management of Utilis.

The Development Department is responsible for the operational establishment and maintenance of the technical controls necessary to comply with the requirements of this policy and supporting acts by adhering to the "privacy by design" principles.

The Management Board of Utilis is responsible for monitoring and interpreting regulations in the field of privacy and providing legal support to the operation of the personal data management system.

The Information System Security Manager is responsible for supervising the application of personal data protection measures and providing professional support in his/her field to the work of the personal data management system.

Keeping records of personal data processing activities

Utilis is obliged to establish and maintain records of personal data processing activities and to appoint a responsible person for each processing and type of personal data. The responsible person is obliged to ensure that only personal data for the processing of which there is an appropriate consent, legal basis or business need are included in the processing.

The Personal Data Controller (VOOP) is responsible for creating records of personal data processing activities and updating them in accordance with changes in business processes and the Utilis information system.

Assessment of the impact of the envisaged processing operations on the protection of personal data

If it is certain that a personal data breach could cause a high risk to the data subject, the controller is obliged, in consultation with the Personal Data Controller (TOOP), to carry out an impact assessment of the envisaged procedures for the protection of personal data.

Impact assessment of the envisaged procedures for the protection of personal data DPIA – Data Protection Impact Analysis) is carried out in accordance with the risk management methodology.

Rights of data subjects and keeping records of data subject requests

Data subjects (owners of personal information) must be given the right to access information about what personal data Utilis holds about them and what is the purpose of the processing. Utilis must enable the data subject to correct inaccurate and complete missing personal data, and the possibility of denying the right to process their data when the processing is based on the data subject's consent.

At the request of the data subject, personal data provided on the basis of consent must be deleted from all Utilis information systems and third-party information systems to which Utilis has provided access to this data. The data subject has the right to the portability of his/her personal data. At the request of the data subject, his personal data must be provided in electronic form.

The process of managing data subject requests in accordance with their rights will be prescribed by a special internal act – procedure. The responsibility for the implementation of the data subject request process lies with the Personal Data Controller (VOOP).

Requests related to the rights of data subjects can be submitted to the E-mail address: szop@utilis.biz

Managing data subject consents

For all processing of personal data of data subjects that are not based on legal or regulatory acts, direct contracts with data subjects or the legitimate interest of Utilis, it is necessary to ensure the process of managing the consent of the data subject. Such processing is based on the explicit consent of the data subject, whose record must be kept within the Utilis information system. This entails keeping a register of consents for such processing.

The responsibility for the process of managing the consent of the data subject is assigned to the personal data controller (VOOP).

Personal data breach management

Utilis will establish and maintain procedures for responding to incidents (breaches) related to personal data breaches within Utilis and with third parties to whom Utilis has provided or who have provided personal data to Utilis.

Utilis will establish and maintain a liability structure for reporting personal data security breaches.

Utilis will establish and maintain measures for the detection of unauthorized access to personal data and leakage of personal data from the information system.

In the event of a breach of personal data security, Utilis will notify the competent authority (Personal Data Protection Agency) without delay, and no later than 72 hours after the incident is detected. In the event of a personal data leak, Utilis will also notify the data subjects whose data has been compromised if this is reasonably practicable.

The process of managing personal data breaches (incidents) of data subjects is prescribed by a special internal act – the Ordinance on Incident Management. The Personal Data Controller (TOOP) is responsible for implementing the process of managing personal data breaches of data subjects in Utilis.

Final and transitional provisions

The policy enters into force and applies on the day of its adoption. The owner of this policy is the personal data controller (VOOP) and is responsible for checking it and updating it if necessary at least once a year.