PRIVACY POLICY

Effective: 01.05.2018.

Modified: 01.09.2026

Content

1. Introduction

This Privacy Policy is issued by Swicon Zrt. to govern its data management activities. The policy is regularly updated to ensure continuous compliance with applicable national and European Union legislation. The current version of the Privacy Policy is available on the website https://swicon.com and is also available in printed form at the reception.

2. Data controller's information

Name of the Data Controller: **SWICON Trading and Services Company Limited by Shares** (hereinafter referred to as SWICON)

Registered office: **1031 Budapest, Záhony utca 7.**

Phone: +36 (1) 883-9860

Email: adatvedelem@swicon.com

Website: https://swicon.com

Company registration number: **01-10-046053**

The person who coordinates data protection activities, the so-called data protection officer:

Madarassy Law Office

3. Purpose of the Code

The purpose of this Privacy Policy is to set out the main rules, information, and principles concerning the processing of personal data by SWICON.

The purpose of this Privacy Policy is primarily to ensure that SWICON complies with the data protection provisions of the applicable legislation, in particular, but not limited to

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information,
- REGULATION (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation)
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers,
- Act CXXXIII of 2005 on the rules of personal and property protection and private investigation,
- the provisions of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activities.

4. Scope of the Code

4.1 Temporal scope

These Rules, as an amendment to the original document valid as of 1 May 2018, are effective as of 1 September 2021.

4.2 Personal scope

The scope of these rules covers

- the Data Controller (SWICON)
- the Employees and Partners of the controller; and
- any other natural person whose data are affected by processing operations covered by this Policy.

4.3 Material scope

This Policy applies to the processing of personal data carried out in any of the Data Controller's departments, whether carried out electronically and/or on paper.

5. Information on data management

The data controller is obliged to inform data subjects about the processing of their personal data.

The privacy notices in the annexes form an integral part of this Policy. The notices contain detailed information on the relevant information concerning each processing operation, such as a description of the processing activity and process, the identity of the data subjects, the scope of the data processed, the foreseeable retention period, the legal basis, and the purposes of the processing. The notices shall include the rules applied to ensure data security, the rights of data subjects, and their means of enforcing their rights.

This Privacy Policy is only valid together with this information.

6. Basic principles of data management

Personal data:

- shall be handled in a lawful, fair, and transparent manner for the data subject ("lawfulness, fairness and transparency");
- collected only for specified, explicit, and legitimate purposes ("purpose limitation");
- shaoo be adequate and relevant for the purposes for which the data are processed and limited to what is necessary ("data minimisation");
- shall be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are erased or rectified without undue delay ("accuracy");

- shall be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed ("limited storage");
- shall be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage ("integrity and confidentiality"), by implementing appropriate technical or organizational measures.

The controller is responsible for compliance with all the above and must be able to demonstrate such compliance ("accountability").

7. Responsibilities

SWICON has kept a register of its data processing activities, which contains the data processing activities and related information (name and purpose of the data processing activity, data subjects, data source, data types, basis for data processing (e.g. consent, legitimate interest of the organisation, law), storage period, storage method, data transfer address labels (if any)). For all data management activities, we have identified a responsible person who can take substantive decisions regarding data management.

The data management activities we carry out in the course of our business (e.g. informing data subjects, obtaining consent) are built into our processes.

Within the SWICON organization, the personal data processed may be accessed and used only by employees of the department concerned, to the extent and for the time necessary for the performance of the task, provided that the case cannot be processed without access to the personal data.

SWICON is responsible for ensuring that all its employees who handle data are familiar with the provisions of this policy. Compliance with the provisions of the policy (usually in conjunction with integrated management system audits) shall be regularly monitored.

8. Safeguarding the rights of data subjects

Data subjects can exercise their rights by notifying through the channels set out in the privacy notices. Requests will be dealt with by the Data Protection Officer. They will involve the data controllers involved in the processing in the execution of the request.

9. Data security

Provisions relating to data protection and security are set out in the SWICON Information Security Policy.

10. Incident management

10.1 The concept of a personal data breach

A data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed.

10.2 Procedure in the event of a data breach

A data breach may cause physical, material, or non-material damage to natural persons if not addressed in an appropriate and timely manner. Such harm may include, inter alia, loss of control over their personal data or restriction of their rights, discrimination, identity theft or misuse, financial loss, damage to reputation, etc.

10.2.1. Announcement

It is the data controller's responsibility to notify the NAIH as soon as it becomes aware of the data breach without undue delay and, if possible, within 72 hours at the latest. If the notification cannot be made within 72 hours, the notification must state the reason for the delay and the required information may be provided in detail without further undue delay.

The notification shall include at least

- describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and the categories and approximate number of data subjects affected by the breach;
- state the name and contact details of the contact person who can provide further information;
- explain the likely consequences of the data breach;
- describe the measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

Where the incident is unlikely to pose a risk to the rights and freedoms of natural persons, the announcement may be waived.

10.2.2. Notification

In the event of a likely high risk to the rights and freedoms of natural persons, the controller shall also inform the data subjects without undue delay in order to enable them to take the necessary precautions. The information provided to the data subject shall contain the information described in point 10.2.1 in an intelligible form in relation to the announcement to be made to the NAIH.

Information to data subjects should be provided as soon as reasonably practicable, in close cooperation with the supervisory authority and in accordance with guidance given by it or other relevant authorities, such as law enforcement authorities.

Data subjects shall be informed using the model in Annex 4.

The data subject need not be informed if any of the following conditions are met:

- the controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorized to access the personal data;
- the controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to exist;
- the information would require a disproportionate effort. In such cases, the data subjects should be informed by means of publicly disclosed information or by a similar measure that ensures that the data subjects are informed in an equally effective manner.

Responsibilities

Any employee of the controller who becomes aware of a data breach must immediately notify the Data Protection Officer.

The Data Protection Officer and the IT Manager will ensure that the tasks set out in point 10.2.1 are carried out and will record the incident (Annex 5).

In addition, the DPO and the IT Manager shall promptly ensure that the relevant staff of the controller take all possible steps to restore the security and lawfulness of the personal data concerned.

Annex 1 : PROCESSING OF PERSONAL DATA OF EMPLOYEES

Annex 2: PROCESSING OF PARTNERS' PERSONAL DATA

Annex 3: PROCESSING OF PERSONAL DATA OF RESPONDENTS

Annex 4: TALENTBEE.SWICON.COM DATA PROTECTION INFORMATION

Annex 5: GETFLOWPLUS.HU DATA PROTECTION INFORMATION

Annex 6: NOTIFICATION OF DATA PROTECTION INCIDENT

Annex 7: INCIDENTAL DATA RECORD

Annex 6: Data breach notification

NOTIFICATION OF A PERSONAL DATA BREACH

SWICON Kereskedelmi és Szolgáltató Zártkörűűen Működő Részvénytársaság, as Data Controller (Registered office: **1031 Budapest, Záhony utca 7.,** Company Registration Number: **01-10-046053,** Phone: +36 (1) 883-9860, Email: adatvedelem@swicon. com, Representative: **Madarassy Law Office (DPO)**)

informs you of:

On the day of....., an incident involving your personal data has occurred.

Description of events:	
Categories and approximate number of persons concerned:	
Categories and an approximate number of data concerned:	
The likely consequences of the incident:	
Actions taken or planned to remedy the incident:	

Date: .....

……..

signature

Annex 7: Data Protection Incident Register

Data protection incident record

Person responsible for keeping the register: the Data Protection Officer in charge

Date of incident	Description of the incident	Categories of persons concerned	Impact of the incident	Actions taken	date of notification (NAIH)	Date of notification (persons concerned)