DATA PROCESSING POLICY

Effective from: 30/04/2024

Table of contents

Introduction

This Privacy Policy is issued by Digital Service Group Kft. to govern its data management activities. The Policy is regularly updated to ensure continuous compliance with current national and European Union legislation. The current version of the Privacy Policy is available on the website http://digitlservicegroup.com and in printed format from the Executive Director.

Details of the data controller

Designation of the data controller: Digital Service Group Kft.
Registered office: 1126 Budapest, Dolgos utca 2. IV. ép. 2. em. 11. ajtó
E-mail: hunor.tollas@digitalservicegroup.com
Website: http://digitalservicegroup.com
Company registration number: 01 09 403370
The staff member overseeing data protection activities (Data Protection Officer): Hunor Tollas

Purpose of the Policy

The purpose of this Data Processing Policy is to set out the main rules, information and principles regarding the processing of personal data by Digital Service Group Kft..
The purpose of this Privacy Policy is primarily to ensure that Digital Service Group Kft. complies with the data protection provisions of applicable law, in particular, but not limited to

1. Act CXII of 2011 on the right to informational self-determination and on the freedom of information
2. 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)
3. Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers,
4. Act CXXXIII of 2005 on the rules of personal and property protection and private investigation,
5. the provisions of Act XLVIII of 2008 on the Basic Conditions and Certain Limitations of Economic Advertising Activities.

Scope of the Policy

Temporal Scope

These Rules shall be in force from 30 April 2024 until revoked.

Personal Scope

The scope of this Policy covers

1. the Data Controller (Digital Service Group Kft.)
2. the Data Controller's Employees and Partners; as well as
3. any other natural person whose data is affected by processing operations covered by this Policy.

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.

Information on data management

The 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 privacy notices provide detailed information about each data processing activity, including the description of the data processing operations and procedures, identification of the data subjects, the scope of the processed data, the anticipated retention period of the data, the legal basis, and the purposes of the data processing The privacy notices include the rules applied to ensure data security, as well as the rights of the data subjects and the means of enforcing those rights.
This Data Processing Policy is valid only in conjunction with this information.

Fundamental principles of data management

Personal data:

1. its management shall be lawful, fair and transparent for the data subject ("lawfulness, fairness and transparency");
2. its collection shall be only for specified, explicit and legitimate purposes ("purpose limitation");
3. shall be adequate, relevant and limited to what is necessary for the purposes for which the data are processed ("data minimisation");
4. 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");
5. shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("limited storage");
6. its management shall be carried out in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage ("integrity and confidentiality"), by implementing appropriate technical or organisational measures.

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

Liabilities

Digital Service Group Kft. has prepared 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, recipients of data transfers (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 our business (e.g. informing data subjects, obtaining consent) are built into our processes.
Within the organisation of Digital Service Group Kft., only employees of the department concerned may access and use the personal data processed - to the extent and for the period necessary for the performance of the task - provided that without access to the personal data, the case cannot be processed in substance.
The CEO of Digital Service Group Kft. is responsible for ensuring that all employees who handle data are familiar with the provisions of this policy. Compliance with the provisions of the code should be regularly monitored (usually in conjunction with audits of the integrated management system).

Ensuring the rights of data subjects

Data subjects can exercise their rights by notifying us through the channels set out in the privacy notices. Requests will be dealt with by the Data Protection Officer. It shall involve those responsible for the processing in complying with the request.

Data security

The provisions relating to data protection and security are set out in the Information Security Policy of Digital Service Group Ltd.

Management of incidents

Definition of a Data Breach

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

Procedure in case of a personal data breach

A personal data breach may cause physical, material or non-material damage to natural persons if not addressed in an appropriate and timely manner. Such damage may include loss of control

over their personal data or restriction of their rights, discrimination, identity theft or misuse, financial loss, damage to reputation, etc.

Report of data breach

It is the data controller's responsibility to notify the Hungarian National Authority for Data Protection and Freedom of Information as soon as it becomes aware of a personal 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 instalments without further undue delay.
The notification shall include at least

1. the description of 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;
2. the name and contact details of the contact person who can provide further information;
3. the description of the likely consequences of a data breach;
4. the description of the measures taken or envisaged by the Data Controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

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

Notification

If the data protection incident is likely to pose a high risk to the rights and freedoms of individuals, the data controller shall inform the data subjects without undue delay, so that they can take the necessary precautions The information provided to the data subject must include the information described in point 9.2.1 in an easily understandable form for the notification to be made to the Hungarian National Authority for Data Protection and Freedom of Information.
Notification of the data subjects must be carried out as soon as possible within reasonable limits, in close cooperation with the supervisory authority, and following any guidance provided by it or other relevant authorities, such as law enforcement agencies.
Data subjects shall be informed using the template in Annex 4.
The data subject need not be informed if any of the following conditions are met:

1. the Data Controller has implemented appropriate technical and organizational protective measures, and these measures have been applied to the data affected by the data protection incident, especially measures such as encryption, which make the data unintelligible to unauthorized individuals
2. the Data 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 likely no longer exists;
3. information would require a disproportionate effort. In such cases, data subjects should be informed through publicly disclosed information, or similar measures should be taken to ensure that data subjects are informed effectively in a comparable manner.

Liabilities

Any employee of the data controller who detects a personal data breach is required to promptly notify the data protection officer.
The Data Protection Officer and the IT Manager shall ensure that the tasks set out in point 9.2.1 are carried out and also record the incident (Annex 5).
In addition, the Data Protection Officer and the IT Manager shall promptly ensure that the relevant staff of the Data Controller take all possible steps to restore the security and lawfulness of the personal data concerned.

Appendix 1: THE PROCESSING OF EMPLOYEES' PERSONAL DATA
Appendix 2: THE PROCESSING OF PARTNERS' PERSONAL DATA
Appendix 3: THE PROCESSING OF APPLICANTS' PERSONAL DATA
Appendix 4: NOTIFICATION OF A PERSONAL DATA BREACH
Appendix 5: DATA BREACH DATABASE

Appendix 4:

NOTIFICATION OF A PERSONAL DATA BREACH

Digital Service Group Kft. as Data Controller (registered office: Dolgos street 2. building IV. 2. floor. 11. door, 1126 Budapest, Hungary; Company Register no: 01 09 403370, Email: hunor.tollas@digitalservicegroup.com, Representative: Hunor Tollas)
informs you of the following:

An incident involving your personal data occurred on .....

Incident Description

Categories and approximate number of persons concerned:
Categories and approximate number of data concerned:
The likely consequences of the incident:

Actions taken or planned to remedy the incident:

Date: ……..

……..……
signature

Appendix 5:

DATA BREACH DATABASE

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

Incident Date	Incident Description	Categories of persons concerned	Impacts of the personal data breach	Actions taken	Date of notification (Hungarian National Authority for Data Protection and Freedom of Information)	Date of notification (individuals concerned)