DUSSER Group
Gép és Gépelem

www.dussergroup.hu | office@dussergroup.hu | Phone: +36 20 809 9151
Headquarters | 7100 Szekszárd, Korsófölde u. 3.

Privacy Policy

Version: 3.0

Budapest, 25 November 2025

Table of contents

1 Introduction

This data protection policy is issued by Gép és Gépelem Kft. for the purpose of regulating its data processing activities. The policy is regularly updated in order to continuously comply with the current domestic and European Union legislation. The current version of the privacy policy can be viewed on the www.dussergroup.hu website and at the data controller's 7100 Szekszárd, Korsófölde u. 3.is also available in printed format at its headquarters.

2 Data of the data controller

Name of data controller: Gép és Gépelem Kft.

Headquarters: 7100 Szekszárd, Korsófölde u. 3.

Company registration number: 17-09-001182

Phone: +36 20 809 9151

Email: office@dussergroup.hu

Website: www.dussergroup.hu

Person responsible for data processing activities: Imre Koloszár and László Éberling managing directors

3 Purpose of the policy

The purpose of this data management policy is to determine the most important rules related to the personal data processed by the Data Controller, as well as the information and principles related to data processing.
The purpose of the data management policy is primarily to ensure that the Data Controller complies with the data protection provisions of the legislation in force, in particular, but not exclusively,

- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information,
- 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)
- 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 Detective Activities,
- the provisions of Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Commercial Advertising Activities.

4 Scope of the policy

4.1 Temporal scope

The previous policy has been revised. These regulations are effective from 25 November 2025 until revoked.

4.2 Personal scope

The scope of this policy shall extend to:

- to the Data Controller
- the Employees and Partners of the Data Controller; as well as
- to any other natural person whose data is affected by data processing subject to this policy.

4.3 Material scope

The scope of this Policy covers the processing of personal data in any organisational unit of the Data Controller, regardless of whether it is carried out electronically and/or on paper.

5 Information on data processing

The data controller is obliged to inform the data subjects about the processing of their personal data. The privacy notices contained in the annexes are an integral part of this policy. The information sheets contain in detail the important information related to each data processing, such as the description of the data processing activity and the process, the name of the data subjects, the scope of the data processed, the foreseeable duration of the data retention, the legal basis and purposes of the data processing. The information contains the rules applied to ensure the security of data, the rights of the data subjects and the possibilities of enforcing their rights.
This Privacy Policy applies only in conjunction with this information.

6 Basic principles of data processing

Personal data:

- be dealt with lawfully, fairly and in a transparent manner for the data subject ('lawfulness, fairness and transparency');
- it may only be collected for specified, explicit and legitimate purposes ('purpose limitation');
- they must be appropriate and relevant to the purposes for which the processing is carried out and must be limited to what is necessary ('data minimisation');
- be accurate and, where necessary, up-to-date; all reasonable measures must be taken to ensure that personal data that is inaccurate in relation to the purposes for which the processing is carried out is erased or rectified without delay ("accuracy");
- it must be stored in a form that allows the identification of data subjects only for the time necessary to achieve the purposes for which the personal data are processed ("limited storage");
- it shall be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage to the data, using appropriate technical or organisational measures ('integrity and confidentiality').

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

7 Responsibilities

Within the organisation of the Data Controller, the processed personal data may only be accessed and used by the employees of the organisational unit involved in the case to the extent and for the time necessary for the performance of the task, provided that the case cannot be prosecuted on the merits without the knowledge of the personal data.
The job descriptions of employees must include the tasks related to the processing of personal data, with special regard to the provision of information on data processing, the obtaining of declarations of consent, the management of records, the keeping of information on the processed data up-to-date, and the procedure related to incidents.
The Data Controller is responsible for ensuring that all employees performing data processing are familiar with the provisions of this policy. Compliance with the provisions of the Code must be checked regularly.

8 Security

The provisions related to the security of data are contained in the Information Security Policy of the Data Controller.

9 Incident management

9.1 The concept of a data breach

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

9.2 Procedure in the event of a data breach

A personal data breach can cause physical, material or non-material damage to natural persons in the absence of appropriate and timely measures. Such damage may include, but is not limited to, loss of control over their personal data or restriction of their rights, discrimination, identity theft or misuse, financial loss, damage to reputation, etc.

9.2.1 Announcement

It is the duty of the data controller to report it to the National Authority for Data Protection and Freedom of Information (NAIH) without undue delay and, if possible, within 72 hours at the latest, as soon as it becomes aware of a personal data breach. If the notification cannot be made within 72 hours, the reason for the delay must be indicated and the required information may be communicated 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, as well as the categories and approximate number of data affected by the breach;
- the name and contact details of the contact person who provided further information should be communicated;
- the likely consequences of the personal data breach should be described;

- the measures taken or planned by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences resulting from the personal data breach, shall be described.

If the incident is not likely to entail a risk to the rights and freedoms of natural persons, the notification may be waived.

9.2.2 Notice

In the event that the personal data breach is likely to entail a 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 precautionary measures. The information provided to the data subject shall contain the information described in Section 9.2.1 in relation to the notification to be made to the NAIH in a comprehensible form.

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

Those concerned shall be informed using the model in Annex 3.

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

- the controller has implemented appropriate technical and organisational protection measures and those 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 incomprehensible to persons who are not authorised 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;
- information would require a disproportionate effort. In such cases, the data subjects should be informed by means of publicly published information or a similar measure should be taken to ensure that the data subjects are equally effectively informed.

9.2.3 Responsibilities

Any employee of the Data Controller who detects a personal data breach shall immediately notify the person responsible for the data processing activity.

The person responsible for the data processing activity shall ensure the performance of the tasks specified in Section 9.2.1 and shall register the incident (Annex 4).

In addition, the person responsible for the data processing activity shall immediately take measures to ensure that the relevant employees of the data controller take all possible steps to guarantee the restoration of the security and lawful processing of the personal data concerned.

Annex 1: Privacy Policy – Gépés Gépelem Kft.

Annex 2: Data breach notification

The company of Gép és Gépelem Kft. (Headquarters: 7100 Szekszárd, Korsófölde u. 3., Company registration number: 17-09-001182, Representative: ... Managing Director, Phone: ..., E-mail: ... @dussergroup.hu, Website: www.dussergroup.hu) as Data Controller
notifies you of:

…….. incident involving your personal data.

Description of the events:

Categories and approximate number of data subjects:

Categories and approximate number of data concerned:

Probable consequences of the incident:

Measures taken or planned to remediate the incident:

Beget:……

……
signature

Annex 3: Data Protection Incident Record

The person responsible for keeping the register is:

Incident Time	Incident Description	Categories of stakeholders	Effects of the incident	Measures taken	Date of notification (NAIH)	Date of notification (data subjects)

Annex 4: Balancing of interests test

Data processing activity:

Reasons for taking the test:

The..... (as data controller) in the .... personal data.

This data processing

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Information Act),

and 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, GDPR):

Article 6(1)(f) of the GDPR: processing *is necessary for the purposes of the legitimate interests pursued by* the controller or by a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular if the data subject is a child.

Section 6 (1) b) of the Information Act, is *necessary for the purpose of enforcing the legitimate interest of the data controller or a third party*, and the enforcement of this interest is proportionate to the restriction of the right to the protection of personal data.

We carry out the balancing of interests test in order to determine whether our legitimate interest on which the data processing is based is proportionate to the restriction of the rights of the person affected by the data processing.

The test was carried out on the basis of the criteria set out in WP29 Opinion 06/2014 (WP217), NAIH Decision No. 2015/515/H, and the NAIH's recommendation on the data protection requirements of prior information.

1. Legitimate interest of the data controller

Description of legitimate interest:

Assessment **of the significance of** legitimate interest:

☐ 1 - minor

☐ 2 - medium significant

☐ 3 - very significant

2. Impact on stakeholders

List of possible effects	Probability **of occurrence** (low/high)	Severity of consequences (low/high)

Criteria to be assessed to determine severity:

Number of people affected:

Nature of the data (whether it is sensitive data):

Is the data publicly available:

How the data is processed:

In relation to data processing, the data subject may have the following reasonable expectations:

Status of the data controller:

Status of the data subject:

Based on the above criteria, **the significance of the impact on the affected** persons is assessed:

☐ 1 - minor

☐ 2 - medium significant

☐ 3 - very significant

3. Safeguards

In order to reduce or eliminate potential negative effects on the data subject, we will take the following measures/provide assurances:

4. Result of the balancing of interests

Beget:

GUIDE TO THE TEST

The "legitimate interest" as a legal basis may support the lawfulness of data processing if the data controller can prove that this legitimate interest (whether its or that of another third party) is more important than the rights and interests of the data subject(s) endangered/violated by the data processing.

This test serves to enable the data controller to assess in advance whether the legal basis of legitimate interest is applicable in the given case, to make an informed decision in relation to the data processing and to provide the data subjects with information in a documented form.

1 Legitimate interest

3 **criteria** to consider before applying this legal basis:

- It must be lawful, i.e. it must not conflict with any legal provision.
- it must be sufficiently clear and precise (i.e. in this point, the legitimate interest must be described in detail and in a comprehensible manner! It is not enough, for example, to say "protection of property".)
- It must be a real and existing interest (you cannot use an access control system or camera surveillance because everyone else does it the same, you have to be able to explain what your specific interest is in it).

Legitimate interests may include, for example: direct marketing, fraud prevention, security or management control of employees, etc.

The nature of **the legitimate interest is important**. For example, it may coincide with the public interest and the interest of the wider community, which tip the scales in a positive direction in the assessment. The same factor may be the broad legal (e.g. non-binding acts, guidelines) or social/cultural recognition of the legality of the interest.

Determination of necessity: Consideration should be given to whether there are other, less invasive tools.

2 Impact on stakeholders

It must be established which fundamental personal rights and freedoms of the persons affected by the data processing and what interests are endangered by the data processing, and what possible effects are to be taken into account in relation to these. Rights/interests of the data subject to be protected, e.g.: right to informational self-determination, personal rights, respect for privacy, etc. The potential impacts on them should be listed and then evaluated.

The assessment must take into account:

- the likelihood of the effect occurring
- the severity of the consequences of the risks that have occurred

To determine the severity, the criteria are, for example:

- Number of people affected
- the nature of the data (whether it is sensitive data)
- whether the data is currently publicly available (this does not rule out the impact, but it should be taken into account!)
- Method of data processing:
    - widely publicized
    - processing and mixing large amounts of data

  - profiling (this can often lead to unexpected and inaccurate conclusions)
- the reasonable expectations of the data subject (what can they expect, what happens to their data?)
- the status of the data controller (employer, multinational company, market leader, etc.) and the data subject (child, employee, student, patient, etc.).

Both the positive and negative effects must be taken into account, as well as the negative effects (on others) that the non-processing may have.

The range of possible negative effects is wide. *E.g.: exclusion, discrimination, damage to the reputation of the person concerned, deterioration of their negotiating position, or even irritation and anxiety can be included here.*

The goal is not to eliminate all negative effects! Disproportion must be eliminated.

To be assessed on a scale of 3:

- If, on the basis of the above, we have assessed the rights of the endangered data subjects with a higher number than our own legitimate interest, then the legal basis does not stand, and it is necessary to apply a sufficient number and quality of safeguards to eliminate the disproportionateness. In the event of a major deviation, the test does not even need to be continued, and the legal basis cannot be applied.
- If the two values are the same, the test can be continued.
- If our interests are considered more significant, the test must still be carried out to the end.
- It is possible to process data on the basis of a minor interest, but only if the rights at risk are also of minor importance. The test must also be performed in this case.

3 Fuses

The extent of the disproportion can be adjusted by providing safeguards.

Such collateral can be, for example:

- strict limits on the amount of data collected
- Immediate deletion of data after use
- technical and organisational measures to ensure functional separation
- Proper use of anonymization techniques
- Aggregating your data
- privacy-enhancing technologies
- increased transparency, accountability, provision of additional information
- Possibility to object to data processing
- steps taken to ensure the portability and accessibility of data.

4 Result of the balancing of interests

Finally, the decision made on the basis of the above must be clearly described. The factors taken into account must be summarised and a statement must be made as to whether or not the legal basis can be applied as a result of the test.