DATA PROTECTION POLICY

BitNet Group Kft

Company Name	BitNet Group Kft
Registered Office	Budapest, Hungary
Business Activity	Mobile Application Development, Web Programming & Custom Software
Website	https://bitnet.hu
Document Owner	[Data Protection Coordinator / Management]
Classification	Internal – Confidential

Version History

Version	Date	Author	Chapter	Description
1.0	[Date]	[Initials]	All	Initial version

Approval

	Function	Name / Signature	Date
Prepared by	Data Protection Coordinator	[Name]	[Date]
Reviewed by	[Function]	[Name]	[Date]
Approved by	Managing Director	[Name]	[Date]

Table of Contents

1. Introduction

Since 25 May 2018, 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 (the "General Data Protection Regulation" or "GDPR") has been directly applicable across all Member States of the European Union, including Hungary.

BitNet Group Kft ("the Company") is committed to ensuring that the personal data it processes is handled in full compliance with the GDPR, the Hungarian Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the "Info Act"), and all other applicable data protection legislation.

Established in 2003, the Company is a provider of mobile application development, web programming, and custom software services, with a track record of over 150 completed projects and 1.8 million app downloads. In the course of its operations, the Company collects and processes personal data of various categories of data subjects, including:

- Current and former employees
- Job candidates and applicants
- Client contacts (project managers, technical contacts, billing contacts)
- Website visitors and prospective clients
- Suppliers and business partners

Additionally, in its capacity as a Data Processor, the Company develops applications and software systems for clients that may involve accessing, handling, or processing personal data belonging to the clients' own data subjects, including end-users of the applications developed.

2. Purpose and Scope

2.1 Purpose

This Data Protection Policy ("the Policy") is an internal governance document that sets out the principles, rules, and organisational framework through which the Company ensures compliance with applicable data protection laws. It is designed to:

- Establish the data protection principles and commitments of the Company;
- Define roles and responsibilities for data protection;
- Provide an overview of processing activities and their legal bases;
- Describe the rights of data subjects and the procedures for handling requests;
- Set out security measures for the protection of personal data;
- Define data retention periods aligned with Hungarian legal requirements;
- Establish breach notification procedures;
- Incorporate privacy by design and by default principles into the software development lifecycle;
- Address the applicability of Records of Processing Activities and Data Protection Impact Assessments; and
- Institute an ongoing compliance review mechanism.

2.2 Scope and Applicability

This Policy applies to all systems, applications, databases, devices, people, and processes that are part of or interact with the Company's information systems. This includes all

employees, management, contractors, consultants, suppliers, and other third parties who have access to personal data processed by the Company.

All persons covered by this Policy are hereinafter referred to as "Users". This Policy shall be made available to all Users and forms part of the onboarding documentation for new employees.

3. Definitions

For the purposes of this Policy, the following terms have the meanings set out below:

Personal Data: any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special Categories of Personal Data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Processing: any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Data Controller: the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: the entity which processes personal data on behalf of and under the instructions of the Data Controller.

Sub-Processor: an entity engaged by the Data Processor to carry out specific processing activities on behalf of the Data Controller, subject to the Data Controller's approval.

Data Subject: a natural person whose personal data is processed by the Company.

Consent: any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Data Protection Coordinator ("DPC"): the person designated by the Company's management to oversee data protection compliance on an ongoing basis and to serve as the internal and external point of contact for data protection matters. (See Section 4.)

DPIA: Data Protection Impact Assessment, a process to help identify and minimise the data protection risks of a project or processing activity.

ROPA: Records of Processing Activities, the formal record of all processing activities carried out by an organisation as described under Article 30 GDPR. Not currently required for the Company (see Section 10.1).

NAIH: the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság), the supervisory authority in Hungary.

4. Roles and Responsibilities

4.1 Management

The Managing Director of the Company bears overall responsibility for data protection compliance. Management shall approve this Policy, allocate adequate resources for its implementation, and ensure that data protection is integrated into the Company's business operations and software development activities.

4.2 Data Protection Coordinator

Although the Company is not legally required to appoint a Data Protection Officer (DPO) under Articles 37–39 of the GDPR — as it is not a public authority, does not conduct large-scale systematic monitoring, and does not process special categories of data on a large scale — the Company recognises the importance of having a clear point of accountability for data protection.

Accordingly, the Company shall designate a Data Protection Coordinator (DPC) who shall be responsible for:

- Advising and informing management and all Users of their obligations under data protection legislation;
- Monitoring compliance with the GDPR, the Info Act, and this Policy;
- Overseeing the handling of data subject requests and ensuring timely responses;
- Managing the dedicated data protection email address and ensuring prompt review of all communications received;
- Coordinating data breach assessment, response, and notification procedures;
- Periodically reassessing whether a formal Records of Processing Activities (ROPA) obligation applies and implementing one if required;
- Providing guidance on Data Protection Impact Assessments (DPIAs) when required;
- Overseeing the integration of privacy by design principles into the Company's development lifecycle;
- Conducting or coordinating periodic compliance reviews and audits;
- Delivering or arranging data protection awareness training for all staff; and
- Acting as the primary point of contact for the NAIH and for clients on data protection matters.

This may be a part-time role alongside other duties, given the Company's size. The DPC shall be involved promptly and appropriately in all matters relating to the protection of personal data. The DPC's contact details shall be communicated to all staff and shall be available to data subjects and the supervisory authority.

4.3 All Users

Every User is responsible for ensuring that personal data they access or process in the course of their duties is handled in accordance with this Policy and applicable law. Users must:

- Process personal data only for authorised purposes and in accordance with documented instructions;
- Report any suspected or actual personal data breach to the DPC without delay;
- Forward any data subject request received to the DPC immediately;
- Maintain the confidentiality of personal data and not disclose it to unauthorised persons;

- Apply privacy by design principles when developing software or systems that process personal data; and
- Complete mandatory data protection training as required.

4.4 GDPR Role of the Company

Under the GDPR, the Company operates in a dual capacity:

As Data Controller (Article 24): when processing personal data of its own employees, client contacts, website visitors, prospective clients, and suppliers for its own determined purposes.

As Data Processor (Article 28): when developing software applications for clients, performing maintenance, conducting testing, and providing IT services where client data may contain personal data of the client's own data subjects, including end-users of the applications developed. In this capacity, the Company processes personal data solely on the instructions of the Data Controller (the client) and in accordance with the applicable Data Processing Agreement.

This dual role requires attention to both controller obligations (transparency, lawful processing, data subject rights) and processor obligations (acting only on documented instructions, ensuring appropriate security, maintaining confidentiality, supporting the controller's compliance).

5. Data Protection Principles

The Company shall ensure that all personal data processing activities comply with the following principles, as set out in Article 5 of the GDPR:

- **Lawfulness, fairness, and transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that inaccurate data is erased or rectified without delay.
- **Storage limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed. The specific retention periods applicable to the Company are set out in Section 11 and Annex 1.
- **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.
- **Accountability:** The Company shall be responsible for, and be able to demonstrate compliance with, all the above principles.

6. Lawful Bases for Processing

The Company shall ensure that every processing activity is based on one or more of the lawful bases set out in Article 6(1) of the GDPR:

- **Consent:** the data subject has given clear consent for processing their personal data for one or more specific purposes.
- **Contract:** processing is necessary for the performance of a contract with the data subject or to take steps at their request prior to entering into a contract.
- **Legal obligation:** processing is necessary for compliance with a legal obligation to which the Company is subject (e.g., Hungarian employment law, tax law, accounting obligations).
- **Vital interests:** processing is necessary to protect the vital interests of the data subject or another natural person.
- **Public interest:** processing is necessary for the performance of a task carried out in the public interest.
- **Legitimate interests:** processing is necessary for the legitimate interests pursued by the Company or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject.

The processing of special categories of personal data is only permitted under the additional conditions set out in Article 9 of the GDPR, including where processing is necessary for carrying out obligations in the field of employment and social security law, or where the data subject has given explicit consent.

Under the Hungarian Equal Treatment Act (Act CXXV of 2003, Section 8), the collection of special categories of personal data for diversity monitoring purposes is not permitted, as it may be deemed discriminatory. The NAIH Employment Guidelines further specify that only job-relevant information may be collected from employees and applicants, excluding data on private life, relationships, family life, or religion.

When acting as a Data Processor, the Company processes personal data solely based on the documented instructions of the Data Controller (client). The lawful basis for processing in such cases rests with the Data Controller.

6.1 Consent Management

Where consent is relied upon as the lawful basis for processing, the Company shall ensure that:

- Consent is obtained through clear, affirmative action and is documented;
- The data subject is informed of their right to withdraw consent at any time, and withdrawal is as easy as giving consent;
- Consent for minors under 16 years of age is obtained or authorised by the holder of parental responsibility; and
- Consent forms are approved by the DPC before use.

Where the Company acts as a Data Processor, the obligation to obtain consent rests with the Data Controller. The Company shall follow the Data Controller's instructions in this regard.

7. Data Subject Rights

The Company respects and upholds the rights of data subjects as provided under the GDPR. Data subjects may exercise their rights by contacting the DPC via the designated data protection email address. Any request received from a data subject, whether by a User or by a third party processing data on the Company's behalf, shall be forwarded to the DPC without delay.

7.1 Procedures for Handling Requests

Upon receiving a data subject request, the DPC shall:

- Verify the identity of the data subject where necessary;
- Log the request and coordinate with the relevant departments to identify all personal data concerned;
- Provide a response in writing within one month of receiving the request;
- Where the request is complex or numerous requests have been received, extend the response period by a further two months, informing the data subject of the extension and reasons within the initial one-month period; and
- Provide the response free of charge, unless the request is manifestly unfounded, excessive, or repetitive, in which case a reasonable fee may be charged or the request may be refused with justification.

All data subject requests and their outcomes shall be logged and documented by the DPC.

7.2 Rights Overview

Right of access (Article 15): Data subjects have the right to obtain confirmation as to whether their personal data is being processed and, if so, access to the data and information about the processing, including the purposes, categories of data, recipients, retention periods, and the source of the data. The data subject may also request a copy of their data in electronic format.

Right to rectification (Article 16): Data subjects may request the correction of inaccurate personal data or the completion of incomplete data.

Right to erasure (Article 17): Data subjects may request the deletion of their personal data where it is no longer necessary for the purpose of collection, where consent is withdrawn, where they object to processing, where data has been unlawfully processed, or where erasure is required by law. This right does not apply where retention is necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims.

Right to restriction of processing (Article 18): Data subjects may request restriction of processing where accuracy is contested, processing is unlawful, the Company no longer needs the data but the data subject requires it for legal claims, or the data subject has objected to processing pending verification.

Right to data portability (Article 20): Data subjects may request to receive their personal data in a structured, commonly used, and machine-readable format, and may request its direct transfer to another controller, where processing is based on consent or contract and is carried out by automated means.

Right to object (Article 21): Data subjects may object to processing based on legitimate interests or public interest, including profiling. The Company shall cease processing unless it demonstrates compelling legitimate grounds that override the interests of the data subject.

Right not to be subject to automated decision-making (Article 22): Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

7.3 Processor Obligations Regarding Data Subject Rights

When acting as a Data Processor, the Company shall assist the Data Controller in fulfilling its obligations to respond to data subject requests. If the Company receives a request directly from a data subject regarding data processed on behalf of a Data Controller, the DPC shall promptly inform the relevant Data Controller and shall not respond to the request directly unless instructed to do so by the Data Controller.

8. Technical and Organisational Security Measures

The Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the likelihood and severity of risk to the rights and freedoms of data subjects.

8.1 Technical Measures

The Company's technical security measures include, but are not limited to:

- Access controls ensuring that systems and data are accessible only by authorised personnel using unique credentials;
- Multi-factor authentication where applicable for access to critical systems;
- Encryption of data in transit and, where applicable, at rest;
- Network security measures including firewalls, intrusion detection, and traffic monitoring;
- Secure software development practices, including code review and vulnerability testing;
- Backup and disaster recovery procedures as documented in the Company's Business Continuity and Disaster Recovery Plan;
- Device security measures including endpoint protection and remote wipe capability;
- Secure configuration of development environments and source code repositories; and
- Regular security updates and patch management.

8.2 Organisational Measures

The Company's organisational security measures include:

- Access control policies ensuring that personal data is accessible only to authorised Users on a need-to-know basis;
- Confidentiality obligations for all employees and contractors;
- Regular data protection awareness training for all staff;
- Secure storage: documents containing personal data must be stored securely; desks cleared of sensitive documents when unattended;
- Prohibition on transferring personal data to personal devices, private email accounts, or unauthorised cloud storage without DPC approval;
- Prohibition on photographing or filming documents, information, or data relating to Company or client activities;
- Secure disposal and deletion procedures for personal data no longer required;
- Separation of development, testing, and production environments to minimise exposure of personal data during the development lifecycle; and
- Incident response procedures as set out in Section 9 of this Policy.

8.3 Privacy by Design and by Default

In accordance with Article 25 of the GDPR, the Company shall integrate data protection considerations into the design of new systems, services, and processes from the outset (privacy by design). By default, only personal data which is necessary for each specific purpose of processing shall be processed (privacy by default). This applies to the amount of data collected, the extent of processing, the period of storage, and the accessibility of data.

8.4 Privacy by Design in the Software Development Lifecycle

Given the Company's core business of mobile application development and custom software, privacy by design shall be embedded throughout the development lifecycle. The following practices shall be applied:

8.4.1 Project Initiation Phase

- A Privacy Checklist shall be completed at the start of each new project to identify whether the application or system will process personal data;
- Where personal data will be processed, the DPC shall be consulted to assess data protection implications;
- The data protection responsibilities of the Company (as processor) and the client (as controller) shall be clarified and documented in the project scope and Data Processing Agreement;
- A preliminary assessment shall determine whether a DPIA is required for the project.

8.4.2 Design and Architecture Phase

- Data minimisation shall be a core design principle: applications shall collect only the personal data strictly necessary for the intended functionality;
- Purpose limitation shall be built into the architecture: data collected for one purpose shall not be technically accessible for incompatible purposes without additional controls;
- Access controls shall be designed into the application from the outset, ensuring role-based access and least-privilege principles;
- Data retention mechanisms shall be incorporated into the design, including automated deletion or anonymisation features where feasible;
- Encryption and pseudonymisation techniques shall be evaluated and applied where appropriate.

8.4.3 Development and Testing Phase

- Real personal data shall not be used in development or testing environments unless strictly necessary and authorised by the DPC and the client;
- Where test data is required, anonymised or synthetic data shall be used wherever possible;
- Source code shall be reviewed for data protection vulnerabilities, including but not limited to: excessive data collection, inadequate access controls, insecure data storage, and logging of personal data;
- Security testing shall include assessment of personal data handling, including injection vulnerabilities, authentication weaknesses, and data exposure risks.

8.4.4 Deployment and Maintenance Phase

- Upon project completion or termination, all personal data provided by the client for development and testing purposes shall be securely deleted or returned in accordance with the DPA;
- Development environments, staging servers, and repositories shall be reviewed and purged of any remaining personal data;
- Ongoing maintenance activities shall follow the same privacy by design principles, and any changes that affect personal data processing shall be assessed for data protection impact.

8.4.5 Documentation

Data protection considerations and decisions made during the development lifecycle shall be documented in the project documentation. This documentation supports the accountability principle and enables the Company to demonstrate to clients that privacy by design was applied throughout the project.

9. Personal Data Breach Management

9.1 Breach Detection and Reporting

All Users must report any suspected or confirmed personal data breach to the DPC without undue delay using the designated data protection email address. The report shall include, to the extent possible:

- A description of the nature of the breach;
- The categories and approximate number of data subjects affected;
- The categories and approximate number of personal data records concerned;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to address the breach and mitigate its effects.

Examples of personal data breaches include, but are not limited to: unauthorised access to systems containing personal data; accidental transmission of data to an unintended recipient; loss or theft of devices or documents containing personal data; malware or ransomware incidents affecting personal data; compromised source code repositories containing personal data; any installation of malicious software on Company devices; and any breach of mandatory security controls that could lead to loss or compromise of personal data.

9.2 Assessment and Response

Upon receiving a breach report, the DPC shall:

- Initiate an assessment to determine whether the incident constitutes a personal data breach under the GDPR;
- Document the assessment, including all facts relating to the breach, its effects, and remedial actions taken;
- Where the incident does not constitute a breach, document the initial assessment for the record; and
- Where the incident constitutes a breach, conduct a risk assessment to determine the likelihood and severity of risk to the rights and freedoms of affected data subjects.

9.3 Notification to the Supervisory Authority (Article 33)

Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Company shall notify the NAIH without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

9.4 Notification to Data Subjects (Article 34)

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall communicate the breach to the affected data subjects without undue delay, in clear and plain language.

9.5 Processor Breach Obligations

When acting as a Data Processor, the Company shall notify the relevant Data Controller without undue delay after becoming aware of a personal data breach affecting client data. The notification obligation to the supervisory authority and to data subjects rests with the Data Controller; however, the Company shall provide all necessary assistance and information as required by the DPA.

9.6 Breach Register

The DPC shall maintain a register of all personal data breaches, including those that did not require notification to the supervisory authority. The register shall record the facts relating to the breach, its effects, and the remedial actions taken. Any updates to the register shall be reviewed and approved by management.

10. Records of Processing Activities and Impact Assessments

10.1 Records of Processing Activities (Article 30)

Under Article 30(5) of the GDPR, the obligation to maintain Records of Processing Activities (ROPA) does not apply to organisations employing fewer than 250 persons, unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or it includes special categories of data or data relating to criminal convictions and offences.

Based on the Company's current size (9–15 employees), nature, and scope of processing activities, the Company is not required to maintain a formal ROPA. Should the Company's circumstances change — in particular through growth in headcount, expansion of processing activities, or the introduction of processing that involves special categories of data — the DPC shall reassess this obligation and implement a ROPA if required.

Notwithstanding the above, the Company maintains adequate internal documentation of its processing activities through this Policy, its Data Retention Schedule (Annex 1), its Privacy Notice, and its Data Processing Agreements with clients.

10.2 Data Protection Impact Assessments (Article 35)

Where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the GDPR requires the Company to carry out a Data Protection Impact Assessment (DPIA) prior to the processing. Based on the Company's current processing activities, no DPIA is presently required.

However, given the Company's role as a software developer, the Company may develop applications for clients that do require DPIA. The DPC shall advise clients on DPIA requirements and assist them as required under the applicable Data Processing Agreement.

Should a DPIA become necessary in the future, the Company shall use the DPIA template published by the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL), which is freely available and widely recognised as a reference methodology across the EU. The DPC shall coordinate the conduct of any DPIA and, where the assessment indicates a high residual risk, shall consult the NAIH prior to processing.

11. Data Retention

11.1 General Principles

Personal data shall be retained only for as long as necessary for the purposes for which it was collected or as required by applicable Hungarian and EU legislation. The Company applies the storage limitation principle, ensuring that personal data is not kept in an identifiable form for longer than necessary.

The specific retention periods applicable to each category of data processed by the Company are defined in Annex 1 – Data Retention Schedule. Annex 1 constitutes the Company's definitive retention schedule and establishes a single applicable retention period for each record type. It is based on the requirements of Hungarian legislation, including but not limited to:

- The Accounting Act (Act C of 2000) – 8-year retention for accounting records;
- The Taxation Act (Act CL of 2017) – tax assessment limitation periods;
- The Labor Code (Act I of 2012) – 3-year limitation period for employment claims;
- The Social Security Act – pension-related document retention;
- The Occupational Safety Act (Act XCIII of 1993) and Ministry of Labor Decree No. 5/1993 – incident records and exposure records;
- NM Decree 33/1998 on Medical Examinations – 30/40-year retention for medical records;
- The Consumer Protection Act (Act CLV of 1997) – customer complaints and correspondence;
- The Civil Code (Act V of 2013) – 5-year general limitation period for civil claims;
- The Commercial Advertising Act (Act XLVIII of 2008) – direct marketing consent records;
- The Attorneys-at-Law Act (Act LXXVIII of 2017) – corporate document retention;
- The Equal Treatment Act (Act CXXV of 2003) – restrictions on special category data collection; and
- NAIH Employment Guidelines – guidance on employee and applicant data processing.

Where multiple retention periods may apply to the same data, the longest applicable period shall be used.

11.2 Retention as Data Controller

The DPC shall be responsible for identifying the applicable retention period for each category of personal data, ensuring retention periods are documented and communicated to relevant departments, coordinating with relevant departments to ensure that personal data whose retention period has expired is no longer used for operational purposes, and ensuring the secure deletion or anonymisation of personal data upon expiry of the relevant retention period.

11.3 Retention as Data Processor

When acting as a Data Processor, the Company shall retain client personal data only for the duration specified in the Data Processing Agreement (DPA) with the respective Data Controller. Upon termination of the DPA or at the Data Controller's instruction, the Company shall either return all personal data to the Data Controller or securely delete it, unless retention is required by applicable law.

11.4 Retention of Development Project Data

Given the Company's core business of software development, particular attention shall be paid to personal data that may reside in development environments, test databases, source code repositories, staging servers, and project documentation. The following principles apply:

- Personal data provided by clients for development or testing purposes shall be treated as processor data and retained only for the duration of the project or as specified in the DPA;
- Upon project completion, handover, or termination, all client-provided personal data shall be securely deleted from development environments, test databases, staging servers, and any backups, unless the DPA specifies otherwise;
- Source code repositories shall be reviewed to ensure no personal data is embedded in code, configuration files, or commit histories;
- Project documentation containing personal data shall be reviewed at project close and purged or anonymised as appropriate; and
- Deletion of project data shall be documented and confirmed to the client.

11.5 Systematic Deletion Procedures

The Company shall implement systematic procedures for the review and deletion of personal data, including:

- Annual review of retained data against the retention schedule;
- Automated reminders or flagging mechanisms where feasible;
- Documented deletion or anonymisation procedures with confirmation records; and
- Secure methods for the destruction of physical documents and the permanent erasure of electronic data.

12. Third-Party and Supplier Management

12.1 Engaging Data Processors

When the Company, acting as a Data Controller, engages a third party that will have access to personal data (such as payroll services, accounting, cloud/hosting providers, IT support, or development tools/platforms), the Company shall:

- Verify that the third party provides sufficient guarantees of compliance with data protection law, including appropriate technical and organisational measures;
- Conclude a Data Processing Agreement in accordance with Article 28 of the GDPR before any processing begins;
- Conduct periodic assessments of the processor's continued compliance, at least annually; and
- Retain a copy of all DPAs under the supervision of the DPC.

No contract involving the processing of personal data on behalf of the Company shall be concluded without the prior written approval of the DPC.

12.2 Sub-Processor Management and Due Diligence

When the Company acts as a Data Processor and engages a Sub-Processor (such as cloud services, development tools, specialist contractors, or third-party APIs), the Company shall:

- Obtain prior general or specific authorisation from the Data Controller;
- Conduct due diligence on the Sub-Processor using the Company's Sub-Processor Due Diligence Checklist, evaluating: privacy policy and data protection practices;

willingness to sign a DPA with appropriate terms; security measures implemented; location of data processing and storage (EU/non-EU); breach notification capabilities; and relevant certifications or compliance attestations;

- Impose the same data protection obligations on the Sub-Processor via a written agreement;
- Maintain a register of approved Sub-Processors and make it available to Data Controllers upon request; and
- Remain fully liable to the Data Controller for the Sub-Processor's performance of its data protection obligations.

During annual reviews, particular attention shall be paid to Sub-Processor activities. If a Sub-Processor fails to fulfil its data protection obligations, the Company shall take appropriate corrective action, including termination of the sub-processing arrangement if necessary.

12.3 International Data Transfers

Personal data may not be transferred outside the European Economic Area (EEA) unless appropriate safeguards are in place as required by Chapter V of the GDPR, such as:

- An adequacy decision by the European Commission;
- Standard Contractual Clauses (SCCs) approved by the European Commission;
- Binding Corporate Rules; or
- An applicable derogation under Article 49 of the GDPR.

Given the nature of IT development work and potential use of international cloud services, development platforms, and collaboration tools, the DPC shall conduct a Transfer Mapping Exercise to identify all services and tools that may transfer data outside the EEA and ensure appropriate safeguards are in place.

When acting as a Data Processor, the Company shall clarify with clients any restrictions on data location and ensure that DPAs include appropriate transfer provisions. When using Sub-Processors in third countries, the Company shall ensure appropriate safeguards (such as SCCs) are in place.

13. Data Protection Contact Point

The Company shall maintain a dedicated email address for all data protection communications: adatvedelem@bitnet.hu.

The DPC shall monitor this email address to ensure prompt review and processing of all incoming communications, including data subject requests, client inquiries regarding data protection, and internal reports.

Employees and contractors shall use this address for any data protection-related requests or reports.

14. Training and Awareness

The Company shall implement a data protection training and awareness programme to ensure all Users understand their obligations. The programme shall include:

- Mandatory data protection awareness training for all new employees as part of the onboarding process;
- Periodic refresher training for all staff, at least annually;

- Role-specific guidance for development staff who may access or handle client personal data during software development projects, including privacy by design principles, secure coding practices, and the use of anonymised or synthetic test data;
- Training on recognising and reporting potential personal data breaches; and
- Documentation of all training delivered, including attendance records.

Training need not be extensive given the Company's size but should cover key GDPR principles, the Company's data protection policies, and practical guidance relevant to each employee's role. The DPC shall be responsible for the design, delivery, and documentation of the training programme.

15. Monitoring, Review, and Continuous Improvement

15.1 Annual Compliance Review

The DPC shall conduct a comprehensive review of the Company's data protection compliance at least once per year. The review shall cover:

- The adequacy and effectiveness of this Policy and all related procedures;
- Whether the conditions triggering a ROPA obligation or DPIA requirement have changed;
- Compliance with retention periods and effectiveness of deletion procedures;
- The results of any DPIAs conducted;
- Training completion rates and awareness levels;
- Any data breaches that occurred during the review period and lessons learned;
- Changes in applicable legislation, regulatory guidance, or supervisory authority decisions;
- The adequacy of third-party, Sub-Processor, and international transfer compliance; and
- The effectiveness of privacy by design practices in the development lifecycle.

15.2 Reporting to Management

Following the annual review, and in cases of urgency (such as a significant data breach), the DPC shall submit a report to the Managing Director covering any identified or potential non-compliance and the corrective actions taken or proposed, significant risks or issues relating to data protection, DPIAs conducted and recommended, new projects or processing activities and their compliance with data protection principles, and recommendations for policy updates or procedural improvements.

15.3 Triggering Events for Policy Review

In addition to the annual review, this Policy shall be reviewed and updated following any of the following events:

- Material changes in applicable data protection legislation or regulatory guidance;
- Significant changes to the Company's business operations, services, or IT environment;
- A significant personal data breach or security incident;
- Findings or recommendations from audits or supervisory authority investigations;
- Changes to the Company's risk profile or threat environment; and

- Any other event identified by the DPC as necessitating a review.

16. Policy Violations

Violations of this Policy shall be investigated by the DPC in coordination with management. Violations may result in disciplinary action proportionate to the severity of the breach, including but not limited to:

- A formal warning;
- Temporary or permanent restriction of access to personal data and information systems;
- Mandatory additional data protection training;
- Termination of employment or contractual relationship; and
- Legal action where appropriate.

17. Document Management

17.1 Effective Date

This Policy is effective as of the date of its approval by the Managing Director.

17.2 Exceptions

Any exceptions to this Policy must be approved in writing by the Managing Director upon the recommendation of the DPC. All exceptions shall be documented, time-limited, and subject to review.

Annex 1 – Data Retention Schedule

The following table establishes the definitive retention periods applicable to all categories of personal data processed by the Company. Where Hungarian legislation prescribes a statutory retention period, that period is applied. Where no statutory period exists, the period is based on applicable limitation periods and regulatory guidance. Where multiple obligations overlap, the longest applicable period has been selected.

This Annex constitutes the Company's authoritative data retention schedule. The DPC shall ensure that personal data is deleted or anonymised in accordance with these periods.

Record Type	Retention Period	Starts From	Legal Basis
A. EMPLOYMENT – PERSONAL DATA			
Personal contact details (address, phone, email)	3 years	Termination of employment	Section 286(1) of the Labor Code
Bank details	3 years	Termination of employment	Section 286(1) of the Labor Code
Formal identification records (full name, occupation)	3 years	Termination of employment	Section 286(1) of the Labor Code
Right to work documentation (work permits, visas)	3 years	Termination of employment	Section 286(1) of the Labor Code
National ID numbers (social security, passport, driver's licence)	3 years	Termination of employment	Section 286(1) of the Labor Code
Work contact details (job title, work email, work phone)	3 years	Termination of employment	Section 286(1) of the Labor Code
Next of kin and emergency contact details	Delete upon termination	Termination of employment	GDPR Art. 5(1)(e) – purpose limitation
B. EMPLOYMENT – LOGS AND ATTENDANCE			
Attendance records	3 years	Termination of employment	Section 134 and Section 286(1) of the Labor Code
Location access records	3 years	Termination of employment	Section 134 and Section 286(1) of the Labor Code
Records of annual leave	3 years	Termination of employment	Section 134 and Section 286(1) of the Labor Code
Workplace incident reports	5 years	Date of incident	Section 64/A Occupational Safety Act; Decree 5/1993 s.5
C. EMPLOYMENT – MEDICAL RECORDS (OCCUPATIONAL)			
Doctors' notes (occupational suitability)	30 yrs; 40 yrs biological exposure	Creation of record	Sections 14(5)-(6) NM Decree 33/1998
Medical reports	30 yrs; 40 yrs biological exposure	Creation of record	Sections 14(5)-(6) NM Decree 33/1998
Records of workplace adjustments	30 yrs; 40 yrs biological exposure	Creation of record	Sections 14(5)-(6) NM Decree 33/1998
D. EMPLOYMENT – PAYROLL AND TAX			
Social security contributions	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Payslips	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Records of deductions from salary	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Records of gross and net salary	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*

Records of statutory (or tax) allowances	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
E. EMPLOYMENT – PENSION			
Dependents and beneficiaries' data	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Pension payslips and payroll cards	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Post-termination elections	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Records of changes to contribution levels	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Records of pension elections (provider)	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
Records of employer matching contributions	8 years	End of financial year	Accounting Act s.169(2); Social Security Act s.99/A*
F. EMPLOYMENT – PERFORMANCE			
Bonus awards	3 years	Termination of employment	Section 286(1) of the Labor Code
Disciplinary records	3 years	Termination of employment	Section 286(1) of the Labor Code
Grievances	3 years	Termination of employment	Section 286(1) of the Labor Code
Performance management records	3 years	Termination of employment	Section 286(1) of the Labor Code
Records of promotion	3 years	Termination of employment	Section 286(1) of the Labor Code
G. EMPLOYMENT – APPLICANT DATA			
Successful applicants – hiring documents	3 years	Termination of employment	Section 286(1) of the Labor Code
Successful applicants – background check	Delete after verification	Completion of check	Labor Code s.11(3), 44/A; NAIH Guidance
Unsuccessful applicants – without consent	Delete upon rejection	Date of rejection	GDPR Art. 5(1)(e); NAIH Guidelines
Unsuccessful applicants – background check	Delete after verification	Completion of check	Labor Code s.11(3), 44/A; NAIH Guidance
Special category data for diversity monitoring	NOT PERMITTED	—	Equal Treatment Act s.8; NAIH Guidelines
H. HEALTH AND SAFETY			
H&S audit reports	5 years	Date of assessment	Occupational Safety Act s.54(5)
Drug/alcohol tests – positive	3 years	Termination of employment	Labor Code s.286(1)
Drug/alcohol tests – negative	1 year	Signature of protocol	Labor Code s.286(1)
H&S policies (records)	3 years	Termination of employment	Labor Code s.286(1)
H&S incident notifications	5 years	Date of incident	Occupational Safety Act s.64/A; Decree 5/1993
H&S investigation reports	5 years	Date of incident	Occupational Safety Act s.64/A; Decree 5/1993
Health/medical tests or surveillance	30 yrs; 40 yrs biological exposure	Creation of record	NM Decree 33/1998 s.14(5)-(6)
Safety representative consultations	3 years	Creation of record	Labor Code s.286(1)
Work arrangements based on health	3 years	Termination of employment	Labor Code s.286(1)

Hazardous substances exposure	10 yrs; 50 yrs carcinogenic	Termination / last exposure	Occupational Safety Act s.63/A(3), 63/B(3)
Risk assessments	5 years	Date of assessment	Occupational Safety Act s.54(5)
Routine employee health documentation	3 years	Termination of employment	Labor Code s.286(1)
I. COMPANY AND FINANCIAL			
Accounting records – financial statements	8 years	End of financial year	Accounting Act s.169(2)
Audit documentation	8 years	End of financial year	Accounting Act s.169(2)
Articles of Association	Permanent; then 10 years	Dissolution of company	Attorneys-at-Law Act s.46(5)-(6); Civil Code s.6:22
Board meeting minutes and resolutions	10 years	Date of creation	Attorneys-at-Law Act s.46(5)-(6); Civil Code s.6:22
Directors' service contracts	5 years	Date claim becomes due	Civil Code s.6:22
Register of members / shareholder records	10 years	Date of creation	Attorneys-at-Law Act s.46(5)-(6); Civil Code s.6:22
Shareholder minutes and resolutions	10 years	Date of creation	Attorneys-at-Law Act s.46(5)-(6); Civil Code s.6:22
J. TAX RECORDS			
Corporate income tax records	8 years	End of financial year	Accounting Act s.169(2); Taxation Act
General tax records	8 years	End of financial year	Accounting Act s.169(2); Taxation Act s.202
Records relating to tax returns	8 years	End of financial year	Accounting Act s.169(2); Taxation Act
VAT / Sales Tax records	8 years	End of financial year	Accounting Act s.169(2); Taxation Act
K. SALES, MARKETING AND CUSTOMER RECORDS			
Customer contracts	5 years	Date claim becomes due	Civil Code s.6:22
Customer complaints log	3 years	Receipt / creation of minutes	Consumer Protection Act s.17/A(7)
Call and correspondence records	5 years	Creation of record	Consumer Protection Act s.17/B(3)
Direct marketing data – customer	Until consent withdrawn	Date consent provided	Commercial Advertising Act s.6(5)
Direct marketing data – prospect	Until consent withdrawn	Date consent provided	Commercial Advertising Act s.6(5)
Data subject request records	5 years	Date claim becomes due	Civil Code s.6:22; GDPR accountability
Lawful bases records (consent, LIA)	5 years	Date claim becomes due	Civil Code s.6:22
L. DATA PROCESSOR RECORDS – SOFTWARE DEVELOPMENT			
Client data under development agreements	As defined in the DPA	Termination/expiry of DPA	Article 28 GDPR; applicable DPA
Test data containing personal data (client-provided)	Delete upon project completion/handover	Project completion or DPA termination	Article 28 GDPR; applicable DPA
Development environment data (databases, staging)	Delete upon project completion/handover	Project completion or DPA termination	Article 28 GDPR; applicable DPA
Source code repos with embedded personal data	Review and purge at project close	Project completion	GDPR Art. 5(1)(e); privacy by design
Project documentation with personal data	Review and purge/anonymise at close	Project completion	GDPR Art. 5(1)(e); applicable DPA

***** For payroll and pension records, the 8-year accounting retention period under the Accounting Act is applied as the standard retention period, as it subsumes the shorter 3-year employment claims limitation. Note: under Section 99/A of the Social Security Act, documents created before 31 December 2024 that are relevant to the determination of pension benefits must be retained for a minimum of 5 years from the date the employee reaches retirement age. Where this results in a longer retention period than 8 years, the longer period applies.*

For records not listed above, the retention period shall be determined by the DPC by reference to the purpose of processing, applicable legal requirements, and the GDPR principle of storage limitation. All retention decisions shall be documented.

Annex 2 – Legislation Reference

The following Hungarian and EU legislation forms the legal framework referenced throughout this Policy and the Data Retention Schedule:

Abbreviation	Full Name	Key Sections	Relevance
The Accounting Act	Act C of 2000 on Accounting	Section 169(2)	Accounting records retention (8 years)
The Taxation Act	Act CL of 2017 on Taxation	Section 202	Tax records retention; limitation periods
The Labor Code	Act I of 2012 on the Labor Code	Sections 11(3), 44/A, 134, 286(1)	Employment records, attendance, limitation
The Attorneys-at-Law Act	Act LXXVIII of 2017 on Professional Activities of Attorneys-at-Law	Sections 46(5), 46(6)	Document retention by legal professionals
The Civil Code	Act V of 2013 on the Civil Code	Section 6:22	General civil claims limitation (5 years)
The Info Act	Act CXII of 2011 on Informational Self-Determination and Freedom of Information	Various	Hungarian data protection law
The Occupational Safety Act	Act XCIII of 1993 on Occupational Safety and Health	Sections 54(5), 63/A, 63/B, 64/A	Work accident records, exposure records
The Occupational Safety Decree	Ministry of Labor Decree No. 5/1993 (XII.26)	Section 5	Work accident recording implementation
The Medical Examinations Decree	NM Decree 33/1998 (VI.24) on Medical Examinations	Sections 14(5), 14(6)	Medical records (30/40 years)
The Social Security Act	Social Security Act	Section 99/A	Pension determination documents
The Equal Treatment Act	Act CXXV of 2003 on Equal Treatment	Section 8	Prohibition of discriminatory data collection
NAIH Employment Guidelines	NAIH Workplace Data Processing Guidelines	Part II, Sections 1.2, 1.3	Employee and applicant data guidance
The Commercial Advertising Act	Act XLVIII of 2008 on Commercial Advertising	Section 6(5)	Direct marketing consent
The Consumer Protection Act	Act CLV of 1997 on Consumer Protection	Sections 17/A(7), 17/B(3)	Customer complaints handling and retention
GDPR	Regulation (EU) 2016/679 General Data Protection Regulation	Art 5.(1)e)	Principles of data minimization and storage limitation

Approval and Signatures

Date: _____

Signature: _____

Name: _____