Gremon Systems Zrt.

General Data Protection Policy

Title	General Data Protection Policy
Company	Gremon Systems Zrt.
Policy version	v1.0
Effective Date	22 August 2018
Review Date	N/A
Owner	János Lóczi, CEO

Gremon Systems Zrt

GENERAL DATA PROTECTION POLICY

Gremon Systems Zrt (Gremon) have implemented this General Data Protection Policy ("**General Data Protection Policy**") in order to comply with legal requirements established by the General Data Protection Regulation ("**GDPR**").

1. Scope. The employees, contractors and consultants of Gremon ("**Employees**") are obliged to comply with this General Data Protection Policy whenever the Employees Process Personal Data in connection with or in the context of the performance of their job responsibilities for Gremon. This General Data Protection Policy does not create any rights for Employees or any rights outside the scope of Gremon's obligations under applicable law. This General Data Protection Policy is confidential and internal to Gremon and shall not create any rights or entitlements of any third parties.

2. Definitions. Capitalized terms shall have the meaning given below or as defined throughout this General Data Protection Policy.

"**Data Subject**" means a natural person to which Personal Data relate.

"**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g., IP-address, cookie tag) or location data. The term Personal Data is very broad under the GDPR. To qualify as Personal Data it is not necessary to combine the name of a natural person with other identifiers of the natural person. See also point 4. for some examples.

"**Processing**" means any use or operation which is performed on Personal Data. That means, anything one can do with Personal Data, such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transfer or otherwise making available, alignment or combination, restriction, erasure or destruction. Please note that Processing can include asking a person for information, capturing information on call details (including call recording), logging and analyzing network traffic and accessing an external database.

3. Objective. This General Data Protection Policy implements the core principles of the GDPR and aims to establish data protection compliance. Any failure to abide by this General Data Protection Policy should lead to ultimately to the termination or dismissal for relevant Employees.

4. Personal Data. Personal Data may include:

- Employee Personal Data, for example, master data (e.g. name, address, phone number, e-mail address, citizenship), organizational data (e.g. department), contractual data (e.g. employment status, contract type), compensation and benefit information, employee attendance data (e.g. time records, paid time off), performance and talent information (e.g. CV, training, performance ratings), information about Gremon assets assigned and used to employee (type of laptops, mobile phone etc., IT-usage data), information contained in emails and other business communication;
- Applicant Personal Data, for example, contact details, CV information, work and education history, skills;

- Business Partner/Vendor Personal Data (in case of natural persons or staff members of Business Partners/Vendors), for example, contact details, information contained in emails and other business communication, bank account details, CRM activities;
- Website/Application User Personal Data, for example, IP-address or other online identifiers, location data, log-file data, contact details.

5. Special Categories of Personal Data. Special Categories of Personal Data or also called sensitive data are Personal Data which may only be processed under further requirements. Special Categories of Personal Data are:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- Genetic data;
- Biometric data (such as electronic fingerprint, iris scan or voice recordings);
- Data concerning health (such as employee's number of sick days, disability status or medical history, incontinency issues);
- Data concerning an natural person's sex life or sexual orientation.

6. Core Data Protection Requirements. Gremon and each of its Employees need to ensure that they always comply with the following Core Data Protection Requirements when Processing Personal Data.

6.1 Key Principles. Each Employee must ensure that Personal Data is

(i) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay ('accuracy');

(v) 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 unless specifically authorized by law; ('storage limitation');

(v) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

6.2 Consent or other Statutory Justification Ground. Gremon shall only Process Personal Data (including making available to others) where the relevant Data Subjects have given through a specific, informed and unambiguous indication their consent to the Processing of their Personal Data, as the case may be, or where a statutory justification ground permits the Processing of the Personal Data. The Processing of Sensitive Personal Data will typically require the explicit consent of the relevant Data Subject.

6.3 Notice. Where applicable, Gremon must notify the Data Subjects prior to the Processing with the following information:

- Identity of Gremon responsible for the Processing of the Personal Data (including contact details);
- Types of Personal Data being Processed;
- Purposes for the Processing of the Personal Data as well as the legal basis (consent or specific statutory justification ground) for the Processing of the Personal Data;
- Where the Processing is based on the overriding legitimate interest of Gremon as statutory justification ground, details on such legitimate interests;
- Recipients or categories of recipients of the Personal Data, international data transfers and reference to the appropriate safeguards and the means by which the Data Subject can obtain a copy of them or where they have been made available;
- Retention period of the Personal Data;
- Data Subject's rights under applicable data protection law, which may include the right of access, the right of erasure, or the right to object;
- Right to withdraw consent at any time without affecting the lawfulness of Processing based on consent before its withdrawal;
- Right to lodge a claim with the Hungarian Data Protection and Freedom of Information Authority;
- Whether the provision of Personal Data by the Data Subject is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences if the Data Subject does not provide such Personal Data,
- Existence of automated decision-making, including profiling, and meaningful information about the logic behind involved, the significance and the envisaged consequences of such processing for the Data Subject (which must be given in a clear and transparent way).

6.4 Purpose Limitation and Retention. The Processing of the Personal Data must be limited to only those activities which are necessary to fulfil the identified purpose(s) for which the Personal Data was collected and which are compatible with the purposes identified in the notice (point 6.3 above). Personal Data must be deleted or anonymize once the stated purposes have been fulfilled and legal obligations met.

6.5 Confidentiality. All Employees must be committed to keeping any Personal Data confidential and not to disclose any Personal Data to unauthorized third parties (within Gremon or outside of Gremon). All Employees must sign the "*Undertaking to Confidentiality and Integrity in the Processing of Personal Data*" of Gremon.

6.6. Disclosure to Service Providers. Service Providers (external third parties providing services to Gremon) may have access to Personal Data. In this case, Gremon must ensure that (i) such access is limited to the Personal Data which is absolutely necessary (need-to-know-principle), (ii) the Service Provider is diligently chosen, considering in particular the technical and organizational security measures provided by the Service Provider, adherence to a recognized Code of Conduct for data protection or an approved Certification for data protection, and (iii) appropriate data processing clauses contained in a relevant service agreement or a separate data processing agreement is in place.

6.7 Data Minimization Principle. The Processing of Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. Any access within Gremon or by third parties must be restricted based on the need-to-know principle.

6.8 Data Subject's Rights. The Data Subjects whose Personal Data is Processed by Gremon may have certain rights against Gremon to request (1) access to their Personal Data, (2) rectification of their Personal Data, (3) erasure of their Personal Data, (4) restriction of Processing of their Personal Data, (5) portability of their Personal Data, (6) objection to the Processing of their Personal Data (including object to profiling), and (7) objection to automated decision making (including profiling). In case Gremon receives such a request, Gremon and its Employees must follow the "*Data Subject Rights Policy*" of Gremon.

6.9 Security/Safeguards. Gremon will take reasonable measures to ensure that Personal Data in Gremon's possession and control is protected against loss, unauthorized access, use, destruction, modification or disclosure and ensure that appropriate technical and organisational security safeguards are in place to protect Personal Data appropriate to the level of risk and sensitivity of the data. Taking into account state-of-the-art, costs, nature, scope, context and purposes of data processing as well as the rights and freedoms of the Data Subjects, this will include in particular the pseudonymization and encryption of Personal Data, measures to ensure confidentiality, integrity, availability and resilience, measures to restore the Personal Data in a timely manner in the event of an incident, and processes for regularly testing, assessing and evaluating the effectiveness of the security measures. Further details are set out in the "*Information Security Policy*" of Gremon

6.10 Data Transfer. Personal Data must not be transferred to countries that do not provide an adequate level of data protection from a European data protection law perspective ("Restricted Countries") unless such transfer complies with data protection adequacy requirements. Restricted Countries are any countries outside of the EU/EEA, with the exception of Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand.

6.11 Data Protection Impact Assessment/Data Protection by Design/by Default. Where a Processing activity, in particular implementing a new technology or IT system, is likely to result in a high risk to the rights and freedoms of the Data Subject, taking in to account in particular the nature, scope, context and purpose of the envisaged Processing activity, a data protection impact assessment must be carried out prior to the launch of the Processing activity. The owner of the Processing activity shall be responsible to comply with the "*Data Protection Impact Assessment Policy*". The level of Gremon s responsibility for such Processing activities is limited if the Processing activities are carried out by Gremon on behalf of a customer.

When developing or considering a new Processing activity, in particular implementing a new technology or IT system, or changing any existing Processing activities, appropriate technical and organizational security measures must be considered prior to implementation. By default, only Personal Data which is necessary for the intended purpose may be collected, processed and used. The owner of the processing activity shall be responsible to comply with the principle of data protection by design and data protection by default. The level of Gremon's responsibility for such Processing activities is limited if the Processing activities are carried out by Gremon on behalf of a customer.

6.12 Keeping Documentation up-to-data. When developing or considering a new Processing activity, in particular implementing a new technology or IT system, or changing any existing Processing activities, the owner of the Processing activity shall initiate the revision of any data protection documentation (such as notices, records of processing activities, data processing and data transfer agreements, accountability management system) to keep such documentation up-to-date.

6.13 Records of Processing Activities. The Processing activities must be documented in a record of processing activities. The owner of the relevant Processing activity is responsible for the completeness and accuracy of the records of processing activities.

6.14 Awareness and Training. All Employees shall receive data protection awareness training to become familiar with this General Data Protection Policy and any supplementing policies, instructions and guidelines.

7. Responsibilities of all Employees. All Employees of Gremon are responsible for complying with this General Data Protection Policy and any supplementing policies, instructions and guidelines. In particular, each Employees shall: (i) meet his or her confidentiality obligations with respect to Personal Data; (ii) Process Personal Data only to the extent necessary to serve the legitimate purpose and to properly perform his or her responsibilities; (iii) undertake any function-related or assigned data protection training; (iv) promptly report any breach of the General Data Protection Policy by contacting his or her direct manager; and (v) ensure that any Personal Data he or she provides to Gremon is true and accurate, and confirm the accuracy of such Personal Data on at least an annual basis.

Failure to meet these responsibilities may result in loss of access privileges and/or labor law sanction or termination of the contractual relationship.

8. Questions

Any questions relating to the General Data Protection Policy should be directed to:

János LÓCZI

Chief Executive Officer

+36 70 310 6609

janos.loczi@gremonsystems.com

This Policy may be updated by Gremon as required.