Gremon Systems Zrt.

Data Subject's Rights Policy

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

Introduction

Gremon has implemented this Policy on Data Subject's Rights under the European Union ("**EU**") General Data Protection Regulation (GDPR), ("**Data Subject Rights Policy**") in order to establish a process for addressing obligations that firms within the Gremon network "**Gremon**") may have as a result of the rights Data Subjects (defined below) may have under the GDPR (and EU member state laws, as applicable) with respect to (1) access to their EU Personal Data (defined below), (2) rectification of their EU Personal Data, (3) erasure of their EU Personal Data, (4) restriction of Processing of their EU Personal Data, (5) portability of their EU Personal Data, (6) objection to the Processing of their EU Personal Data, and (7) objection to automated decision making (including profiling). Where local data privacy or protection law establishes greater protections for EU Personal Data, such local law will apply.

Any failure to abide by this Data Subject Rights Policy may lead to labour law sanctions for the relevant Personnel (defined below), up to and including dismissal where permitted by law.

1. Scope.

This Data Subject Rights Policy establishes a process that all employees, contractors, temporary employees or outside consultants of Gremon ("**Personnel**") are required to follow in case a Data Subject exercises his/her rights under the GDPR. This Data Subject Rights Policy does not create any rights for Personnel or any rights outside the scope of Gremon's obligations under the GDPR and applicable EU member state laws. This Data Subject Rights Policy is confidential and internal to Gremon and does not create any rights or entitlements for any third parties.

2. Definitions.

Capitalized terms should have the meaning given below or as defined throughout this Data Subject Rights Policy.

> "**Data Subject**" means a natural person to which EU Personal Data relates, including employees, contractors, job applicants and individual contacts of corporate customers, suppliers or other third parties.
>
> "**EU Personal Data**" means any information relating to an identified or identifiable natural person who is located in or whose information is hosted, stored, or otherwise Processed in the EU/EEA or controlled by an entity that is located or established in the EU/EEA, even if the Processing does not take place in the EU/EEA. 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.
>
> "**Processing**" means any use or operation that is performed on EU Personal Data, such as collection, recordation, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, transfer or otherwise making available, alignment or combination, restriction, erasure or destruction of EU Personal Data.

3. Process for Responding to Data Subject Rights.

Whenever Personnel receive a request from a Data Subject relating to Data Subjects' rights, the following process should be followed:

Forward the request to Request Responder.

Whenever Personnel receive a Data Subject's rights request, such request should promptly (within 2 business days) be forwarded to the responsible for data protection ("**Request Responder**") so the Request Responder can determine how to address the request in the timeframe allowed by applicable law (see 3.6 below).

Determine whether the request falls under the GDPR.

The Request Responder should determine whether the Data Subject is eligible to request the relevant Data Subject right by determining:

- Is the Gremon that holds/stores and/or controls the relevant EU Personal Data located in the EU/EEA?
- Is the Data Subject located in the EU/EEA (e.g., an EU/EEA resident)?

If the answer to either question is yes, the Request Responder should follow the process set out in this Data Subject Rights Policy. If the answer to both questions is no, the Request Responder should inform the Data Subject that the Data Subject rights under the GDPR do not apply to him/her. This can be done directly to the Data Subject. The remaining steps set out this Data Subject Rights Policy apply only to in-scope requests.

Determine type of request.

The Request Responder should determine the type of category into which the request falls. Data Subjects can (in certain circumstances as detailed below) make the following types of requests with regard to their EU Personal Data:

(1) Access Request[1]
(2) Rectification Request[2]
(3) Erasure Request (Right to be Forgotten)[3]
(4) Restriction Request[4]
(5) Portability Request[5]
(6) Objection Request[6]
(7) Objection to Automated Decision Making[7]

Verification of Request.

The Data Subject should make the request in writing (email is acceptable). If the request initially is oral, the Request Responder should request it in writing. If necessary, the Request Responder should request information from the Data Subject in order to verify the identity of the Data Subject.[8]

Confirm Receipt.

The Request Responder should confirm receipt of the request to the Data Subject in writing (email is acceptable) within five (5) business days after receiving the written request and if appropriate obtain further details on the request, i.e. what data is involved, what purposes are captured.

Respond in Timely Manner.

The Request Responder should respond to any requests within one month after receipt of the request. In exceptional cases and where necessary due to the complexity and number of requests, such time period can be extended by two additional months, in which case the Request Responder should inform the Data Subject of the delay within one month of receipt of the request and provide information about the reasons for the delay. If the Request Responder determines not to act upon the request in the manner requested by the Data Subject, the Request Responder should also respond within one month after receipt of the

[1] GDPR Article 15.
[2] GDPR Article 16.
[3] GDPR Article 17.
[4] GDPR Article 18.
[5] GDPR Article 20.
[6] GDPR Article 21.
[7] GDPR Article 22.
[8] Authenticate current employee through work email or other appropriate means. Authenticate former employee through email on record, home address on record or other appropriate means. Authenticate client contact through email on record.

request to explain why Gremon is not taking action to comply with the request and to advise the Data Subject of his/her right to lodge a complaint with the relevant EU supervisory authority and to seek judicial redress.

Form of Response.

The response should be provided in writing or, where appropriate, by electronic means. If the request was made electronically, the response should be provided electronically, unless otherwise requested by the Data Subject. A response should not be provided orally.

Unfounded or Excessive Requests - Rejection and Fees.

In case a request is clearly unfounded or excessive, in particular because of its repetitive nature, the Request Responder may decide to refuse to act upon the request or, after confirming that local law does not require otherwise, to charge a fee. In either case, the Request Responder should respond to the Data Subject within one month after receipt of the request to explain why Gremon is not taking action to comply with the request or charging a fee to respond to the request and to advise the Data Subject about his/her right to lodge a complaint with the relevant EU supervisory authority and to seek judicial redress.

Request Responses.

The process for responding to each type of Data Subject rights request is set out below:

Access Request. The right of access under the GDPR means that a Data Subject has the right to obtain from Gremon confirmation regarding whether Gremon Processes EU Personal Data about him/her and in such case, obtain certain additional information about such Processing ("**Access Request**"). Specifically, Gremon should provide the Data Subject with a copy of, or access to, the EU Personal Data and the following information:

- The purposes of Processing of the EU Personal Data;
- The categories of EU Personal Data that it maintains about the Data Subject;
- The sources of the EU Personal Data (if not directly provided by the Data Subject) (e.g., former employer, background check provider, marketing lead provider);
- The recipients or categories of recipient to whom the EU Personal Data about the Data Subject have been or will be disclosed and their location (particularly if the recipients are located outside the EU/EEA) (e.g. third party service providers);
- The duration of retention of the EU Personal Data;
- The existence of the right to request rectification or erasure of EU Personal Data or restriction of Processing of EU Personal Data concerning the Data Subject or to object to such Processing;
- The right to lodge a complaint with the relevant EU supervisory authority;
- The technical security measures put in place to safeguard EU Personal Data in case of data transfer outside the EU/EEA; and
- If applicable: the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences thereof for the Data Subject.

Rectification Request. The right of rectification under the GDPR means that a Data Subject has the right to obtain from Gremon without undue delay the rectification (i.e., correction) of inaccurate EU Personal Data about him/her ("**Rectification Request**").

Erasure Request. The right of erasure under the GDPR means that the Data Subject has the right to obtain the erasure or obfuscation of EU Personal Data about him/her in the circumstances described in this section ("**Erasure Request**"). Specifically, a Data Subject has the right to request the erasure of his/her EU Personal Data, except where the retention is required:

(i) to perform a transaction with the Data Subject;
(ii) to fulfill an overriding legitimate grounds for the Processing that is not outweighed by the EU Data Subject's interest(s);

(iii) to comply with an EU or local member state law;
(iv) to establish, exercise, or defend legal claims;
(v) to exercise the right of freedom of expression and information;
(vi) for the performance of a task carried out on public interests grounds; and/or
(vii) for scientific or historical research/statistical purposes.

In addition to erasure or obfuscation of EU Personal Data in response to an Erasure Request, in the absence of a litigation hold or other compelling matter, Gremon should delete EU Personal Data upon the expiration of the relevant retention period in accordance with Record Retention Policy & Schedule.

Restriction Request. The right to restriction under the GDPR means that the Data Subject has the right to request that Gremon restrict (i.e., limit or suspend) the Processing of EU Personal Data in the circumstances described in this section ("**Restriction Request**"). Specifically, Gremon should restrict the Processing of EU Personal Data in the following circumstances:

(i) the Data Subject indicates that the EU Personal Data is inaccurate (at least until Gremon can verify whether the EU Personal Data is in fact inaccurate and needs to be corrected);
(ii) the Data Subject indicates that Processing of the EU Personal Data is unlawful, and the Data Subject opposes the erasure of the EU Personal Data and requests the restriction of its use instead;
(iii) Gremon no longer needs the EU Personal Data for the purposes of the Processing, but it is required by the Data Subject for the establishment, exercise or defense of legal claims; or
(iv) the Data Subject has made an **"Objection Request"**, and the Request Responder is in the process of verifying whether the legitimate grounds of Gremon override those of the Data Subject, so that Gremon can continue with the Processing of the EU Personal Data.

Lifting the Restriction: Gremon may lift the restriction of the EU Personal Data and Process the EU Personal Data for purposes other than storage only with the Data Subject's consent or for the purpose of establishment, exercise or defense of legal claims or for the purpose of the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a EU member state. The Request Responder should inform the Data Subject before the restriction of the Processing is lifted.

Portability Request. The right to portability under the GDPR means that the Data Subject has the right to request that Gremon compile the EU Personal Data the Data Subject has provided to Gremon about him/herself in a structured, commonly used, and machine-readable format, and provide the same to the Data Subject, so that the Data Subject may transmit the data to a third party ("**Portability Request**") where:

(i) The Processing of the EU Personal Data is based on the consent of the Data Subject or on a contract with the Data Subject, and the Processing is carried out by automated means (i.e., through IT systems); or
(ii) The EU Personal Data at issue is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Objection Request. The right to objection under the GDPR means that the Data Subject has the right to object to the Processing of the Personal Data that Gremon holds about him/her ("**Objection Request**"). More specifically,

(i) The Data Subject has the right to object at any time to the Processing of his/her EU Personal Data for purposes of direct marketing (marketing via postal mail, email, telephone call, text message, fax, push notifications), including to the Processing for profiling purposes that relate to direct marketing; and
(ii) The Data Subject has the right to object to the Processing of the relevant EU Personal Data if the legal basis of Processing is "Necessary for the performance of a task carried out in the public

interest or in the exercise of official authority vested in Gremon" (Art. 6(1)(e) GDPR) or "Legitimate Interest/ Balancing of Interests Test" (Art. 6(1)(f) GDPR).[9]

With the exception of Processing for direct marketing purposes, Gremon is not legally obligated to honor the Objection Request if Gremon has compelling legitimate grounds for the Processing of such EU Personal Data that override the interests, rights and freedoms of the Data Subject or if the Processing by Gremon is necessary for the establishment, exercise or defense of legal claims.

To the extent a Data Subject raises a concern upon receiving the response, such concern should be referred to the Office of the General Counsel immediately.

Objection to Automated Decision Making. Data Subjects have the right under the GDPR not to be subject to a decision based solely on automated processing, including Profiling[10], In practice, Gremon rarely (if ever) relies on automated decisions without human review. However, where Gremon makes decisions on an automated basis that may significantly affect the Data Subjects (e.g., job applicant decisions without human review), Gremon should either:

(i) modify the procedure to allow human intervention or review on demand prior to making the decision, or (ii) allow the Data Subject to request not to be subject to the decision, or if Gremon is lawfully permitted to proceed with the automated decision-making in the particular circumstances, allow the Data Subject to request human intervention and/or to contest the decision or express his/her point of view.

This Data Subject Rights Policy may be updated by Gremon as required.

[9] Such Processing can particularly relate to Profiling (see next footnote for definition).

[10] Profiling means any form of automated Processing of EU Personal Data consisting of the use of EU Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.