December 2024

Allot Ltd

Allot GDPR Data Subject Request Protocol

I. PURPOSE

The purpose of this document is to lay out, as required by the EU General Data Protection Regulation (the "**GDPR**" and/or the "**GDPR Regulations**"), the procedure of responding to a data subject's request for the execution of his/her rights under the section *Rights of Data Subjects* , in particular, sections 15-21, of the GDPR Regulations.

The rights covered in this protocol are the right to access personal data, the right of rectification, the right to be forgotten, the right to portability, and the right to restrict processing.

Any action subject to this Protocol must be in accordance with its provisions, and in particular with the process of identification and verification, as set out in Part IV.

This Protocol is divided into 4 parts as follows:

1. Part I Definition of Terms
2. Part II Summary of Rights of Data Subjects under the GDPR Regulations
3. Part III Details of the Prerequisites for the existence of any Relevant Right
4. Part IV Identification and Verification, Communicating with Requesting Party, Miscellaneous

Procedures and documents related to this Protocol:

Database settings document; database system mapping document; data security protocol; permission access procedure; backup and restore protocol.

PART I

II. DEFINITIONS

Company - Allot LTD.

GDPR Regulations - Regulation (EU) 2016/679 (General Data Protection Regulation), in effect since 25 May 2018.

Personal Data - Any information relating to an identified or identifiable natural person stored at a given time in the Company's database.

Requesting Party - The data subject to which the request relates.

Data Security Procedures - Includes all existing data security procedures at the time of review, including the database settings document and the data security protocol.

Database Systems - Infrastructure and hardware systems, types of communication and information security components.

PART II

III. SUMMARY OF DATA SUBJECTS' RIGHTS

1. **Right of access** (GDPR Article 15) The data subject has a right: (1) to receive confirmation from the Company as to whether there is personal data being processed about him/her by the Company. (2) if the answer is yes, to have access to personal data about him/her processed by the Company.

2. **Right to rectification** (GDPR Article 16). The data subject has a right to request the correction and/or completion of personal data regarding him/her, which is incorrect, inaccurate and/or incomplete.

3. **Right to erasure** ('right to be forgotten') (GDPR Article 17). The data subject has a right to request the erasure of his/her personal data. Where the conditions for erasure are met, as explained below, the relevant personal data must be erased without delay.

4. **Right to restriction of processing** (GDPR Article 18). The data subject has a right to stop and/or restrict processing of his/her personal data, subject to the conditions as described below.

5. **Right to data portability** (GDPR Article 20). The data subject has a right to receive the personal data he/she provided the Company, via electronic file in a common format readable by a computer. The data subject has a right to transfer the personal data to another party subject to the conditions detailed below.

6. **Right to object** (GDPR Article 21). The data subject has a right to object to the processing of the personal data about him/her, at any stage, subject to the conditions set out below. Where the objection is to the processing of personal data for direct marketing purposes, no conditions should be attached to the termination of the processing.

PART III

This section sets out the prerequisites for the fulfilment of data subjects' rights as well as the necessary steps for implementation.

The execution of the actions must be carried out in accordance with the provisions of this part and in accordance with the provisions of part IV.

Warning – Personal data must be transmitted to and/or received from the data subject in a secure and encrypted manner, as much as possible, and must only be transmitted to the party requesting the data. In no case should any personal data be transmitted which would infringe on the privacy of other data subjects, for example by identifying them without their explicit consent.

A. Right of access (GDPR Article 15)

Prerequisites for the Exercise of the Right

1. Identification and identity verification of the requesting party, as specified in Part IV.

2. Existence of personal data concerning the requesting party (data subject).

The Company cannot act per the requesting party's request without identification and identity verification.
If the Company doesn't process personal data concerning the requesting party, the Company should inform the requesting party that it has no personal data concerning the requesting party.

Execution – If the prerequisites are fulfilled, the following information must be provided to the requesting party:

1. Confirmation that the requesting party’s personal data is being processed.

2. Access to existing personal data – Each database/information system relevant to the personal data must be inspected. The requesting party must then be provided with a copy of the existing personal data in a common computer-readable electronic file containing the existing personal data.

3. In addition, the following must be provided to the requesting party in a common computer-readable electronic file:

    a. Purposes of processing of the personal data [a fixed format of the processing objectives can be prepared and sent to the requesting party];

b. Relevant personal data categories (information fields) [as above];

c. Recipients of personal data, especially in relation to third countries and/or international organizations [as above];

d. Estimated retention period of personal data or criteria for determining the retention duration [according to Company internal procedure]

e. The data subject must be made aware of his/her rights under the GDPR regulations (regarding the right to be forgotten, correcting the personal data and limiting the processing of personal data about him/her, and the possibility of filing a complaint). The proposed wording is as follows:

Dear Customer/Employee, please note that you have the right to request from us the rectification or erasure of your personal data, or to ask us to stop using it. We will make our best possible effort to respond to your request as soon as possible. For your convenience, and for any request or complaint, please contact us at Privacy@allot.com*

** The relevant authority depending on the data subject geographical location*

f. The sources of personal data on the data subject, where the personal data is not collected directly from him/her;

g. When and if profiling (data subject profile profiling) is performed and/or an automatic decision-making process is conducted in relation to the data subject, then –

details about the process, description of the logic (through decision making and/or profile creation), and significance of the predictable implications of the profile and/or automatic decision making must also be transmitted.

4. Only one copy (as mentioned above, in an encrypted manner) must be forwarded to the requesting party. If the party is requesting more than one copy, payment may be required for reasonable expenses in relation to the matter.

B. Right to rectification (GDPR Article 16)

Prerequisites for the Existence of the Right (cumulative conditions)

1. Validation and identification of the requesting party, as specified in Part IV.

2. Existence of incorrect and/or incomplete personal data – The requesting party must provide references regarding the accuracy of the personal data requested for the update; the requested references must be transmitted by secure and encrypted means.

Execution – If the prerequisites are fulfilled, then the following must be performed:

3. Rectify the incorrect personal data according to the references provided by the requesting party. Where there is no proof of the inaccuracy and/or incompletion of the personal data, the request must be passed on for review by the legal department.

4. Where the request is in relation to the completion of incomplete personal data, the need for completion may and should be considered, depending on the purposes of personal data processing and the need for the integrity of the personal data in light thereof.

5. A request made pursuant to this section must be executed without delay.

6. After the execution is complete, confirmation must be sent to the requesting party that his/her request has been completed.

7. The references that have been transferred for the purpose of rectifying the personal data must be kept for the retention period necessary for legal protection, and used only for the purpose of rectifying the personal data or for legal defense, insofar as this is required.

C. Right to erasure (GDPR Article 17)

Prerequisites for the fulfilment of the Right (except for the identification requirement, the conditions are alternative)

1. Identification and verification of the requesting party, as specified in Part IV.

2. The personal data requested for erasure is no longer needed in relation to the original purposes for which it was collected.

3. When the personal data is collected and/or processed on the legal basis of consent and the requesting party withdraws the consent; here, the personal data should be erased unless its retention is required based on other legal grounds.

4. When the legal bases for the processing of personal data is: (1) a legitimate interest, or (2) necessary for the performance of a task carried out in the public interest, and the requesting party objects to the processing of existing personal data about him/her, and these bases do not override the rights of the data subject.

5. With respect to personal data processed for direct marketing purposes, and the requesting party objects to the processing of the personal data for this purpose.

6. The personal data is unlawfully processed.

7. The personal data must be erased pursuant to a legal obligation in an EU member state, to which the Company is bound.

8. The personal data concerns a person who, at the time of collection, was a minor (aged under 16).

Execution - If the identification and verification requirement is met, and one of the additional conditions listed above is met, then the following steps should be taken:

9. If a general request for erasing personal data is received, the personal data contained in all relevant database systems must be reviewed and classified as necessary and according to the legal basis by which it is processed (express consent, provision of a service, legitimate Company interest, a vital interest of the data subject, a vital interest of the public, *etc.*).

10. The personal data that can be erased should be identified based on the conditions specified above. Special notice should be taken of personal data required for legal protection and/or for the purpose of maintaining a requested service by the requesting party, which should not be erased.

11. Prior to erasure, a secure message must be sent to the requesting party, specifying the following:

    a. Types of personal data identified.

    b. Types of personal data that can and will be erased.

    c. Types of personal data that cannot be erased (if requested to be erased), the reason for which it cannot be erased, and the estimated retention time.

    d. If there is personal data determined suitable for erasure, approval for permanent erasure must be requested and received.

12. After obtaining final erasure approval from the requesting party, the approved personal data must be erased.

13. For personal data that has been requested to be erased and cannot be erased, it must be ensured that moving forward it will only be used for the purpose for which the request for erasure has been denied (e.g., for tax purposes) and will not be used for any other purpose.

14. If the requesting party's personal data has been transmitted to third parties (whether outsourced or otherwise), effort should be made, as far as reasonably possible, to notify the third party of the erasure request received. These notifications and the responses received must be documented.

15. **In any case where an erasure request is received, the removal of the requesting party's contact information from any existing mailing list must be performed.**

D. Right to restriction of processing (GDPR Article 18)

Prerequisites for the fulfilment of the Right (except for the identification requirement, the prerequisites are alternative)

1. Identification and verification of the requesting party, as specified in Part IV.

2. The requesting party raised a complaint about the inaccuracy of the personal data.

3. The processing of the personal data is unlawful, and the requesting party objects to the erasure of personal data and requests processing restriction instead.

4. The Company no longer needs the personal data for the purposes of the processing, but they it is required by the data subject for the establishment, exercise or defence of legal claims.

5. The requesting party submitted a separate request, objecting to the processing of personal data, and the request is pending while the Company's legitimate interests are examined.

Execution - If the identification and verification requirement is met, and one of the additional conditions listed above is met, then the following should be performed:

6. The personal data contained in all relevant database systems must be reviewed and the requesting party's personal data found and processed in the systems must be identified.

Manner of restriction

7. Restricted personal data shall not be processed in any way apart from storage, unless the data subject has given his/her consent for further processing, or if further processing is required for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of an EU Member State. The restriction of processing can be done in several ways, to the Company's choosing – whether by transferring the personal data to a separate database, performing logical separation, limiting user privileges, and the like.

8. In all cases the restricted personal data in the Company's systems should be clearly marked as information restricted for processing.

Duration of restriction

9. If prerequisite (2) above is fulfilled, then processing of the personal data should be restricted for the required time until a decision is made regarding the rectification of personal data.

10. If prerequisite (3) above is fulfilled, then processing of the personal data should be restricted until the legal defect in the personal data processing has been remedied, as much as possible. Otherwise, processing of the personal data must be restricted until its erasure.

11. If prerequisite (4) is fulfilled, then processing of the personal data should be restricted for the time required for the requesting party's legal needs, or until the personal data required has been sent to the requesting party and his/her approval for erasure has been received.

12. If prerequisite (5) is fulfilled, then processing of the personal data should be restricted until a decision on the objection has been issued.

E. Right to data portability (GDPR Article 20)

Prerequisites for the fulfillment of the right (except for the identification requirement, the prerequisites are alternative)

1. Identification and verification of the requesting party, as specified in Part IV.

2. The personal data requested for portability is processed on a legal basis of consent, or for the purpose of fulfilling a contract or providing a service.

3. The personal data requested for portability is processed by automatic means.

Execution - If the identification and verification requirement is met, and one of the additional conditions listed above is met, then the following should be performed:

4. The personal data found in all relevant database systems must be reviewed and the requesting party's personal data found and processed in the systems must be identified.

5. The personal data provided to the Company and contained in its systems must be collected in an electronic file in a common and readable computer format (the "**Data File**") and transmitted to the requesting party in a secure and encrypted manner, as much as possible.

6. At the request of the requesting party, the Company must transfer the Data File to another party, provided that:

    a. Technical capacity exists to perform the transfer.

    b. A notice has been sent to the requesting party stating the other party's details as found by the company.

c. Confirmation was received from the requesting party that the receiving party's details (contact details in particular) were correct, and the transfer was approved by the requesting party.

7. A request for portability does not contradict a request for erasure from the same data subject, and the Company shall not oppose a request for portability due to a request for erasure.

F. <u>Right to object (GDPR Article 21)</u>

Prerequisites for the fulfilment of the Right (except for the identification requirement, the prerequisites are alternative)

1. Identification and verification of the requesting party, as specified in Part IV.

2. The personal data requested for portability is processed on a legal basis of the performance of a task carried out in the public interest or on the legal basis of a legitimate interest.

3. The personal data is processed for direct marketing purposes, including profiling carried out for this purpose.

Execution - If the identification and verification requirement is met, and one of the additional conditions listed above is met, then the following should be performed:

4. The personal data found in all relevant database systems must be reviewed, and the requesting party's personal data found and processed in the systems must be identified.

5. If prerequisite (2) is met, then processing of the personal data being carried out must be stopped, unless:

   a. The Company can demonstrate a legitimate interest prevailing over the requesting party's individual rights.

   b. If the processing is carried out for scientific, historical or statistical purposes and the processing in question is necessary for the performance of a task that is necessary for the public interest.

6. If prerequisite (3) is met, then processing of the personal data must be stopped.

<u>PART IV</u>

<u>Identification and Verification</u>

1. Upon receipt of each request, the first action to be taken is verifying the requesting party's identity.

2. The identity verification must be done by means of identification that will verify the requesting party's identity to a reasonable degree, including –

    a. By using a one-time identification method that is controlled by the data subject as it appears in the Company's systems (*e.g.*, sending a one-time password to the data subject's mobile number as updated in the Company's systems);

    b. By identifying questions based on prior knowledge to which only the data subject has access;

    c. In any other manner which will result in the verification of the requesting party's identification.

3. The identity verification must be documented, including the details, time, and date of the verification.

4. Records of the identity verification must be kept for the length of time required for legal protection.

5. Verification by way of ID card – It is clarified that identification by way of ID card, where the requesting party must provide an ID card for verification of his/her identity, is not recommended, and this verification should be used as a last resort. To the extent that these means are used for identity verification purposes, we recommend encrypting the ID card received by the Company and keeping it for the minimum time required.

6. Where an erasure request is received, it must be made clear in the response to the requesting party that the details of carrying out his/her request and the verification will be retained for the time required for legal defense, and for this purpose only.

Communicating, responding and corresponding with the requesting party

1. Any inquiry by a data subject regarding his/her rights shall always be reported immediately to Privacy@allot.com

2. Any correspondence and/or communication with the requesting party will be with the approval of Company CISO.

3. An initial response, whenever required, will always be for identification and verification purposes.

4. Any transfer of personal data, including identification details and identity verification, will always be carried out in a secure manner, and encrypted if possible.

5. In any response to and/or communication with the requesting party, and before sending a reply and/or personal data to the requesting party, the authorized party shall ensure that the personal data transmitted does not infringe on the privacy of other data subjects.

Miscellaneous

6. Each request received and processed will be documented.

7. **Any request for erasure/correction/restriction of personal data shall be reported by the Company to any third party and/or provider to whom the requesting party's personal data has been forwarded, unless it involves unreasonable effort.**