EVERBRIDGE DATA SUBJECT ACCESS REQUEST PROCEDURES

POLICY DETAIL REPORT

Everbridge Data Subject Access Request Procedures

Owned by Everbridge Legal/Privacy

Description

The purpose of these procedures is to establish a uniform set of instructions for responding to Data Subject Access Requests as provided for in Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and for the purpose of this document, includes the corresponding laws of the United Kingdom including the UK GDPR and Data Protection Act 2018 (collectively, the GDPR).

Versions

- 4.0 **(current version)**: **Active** (published on **2025-10-30**)
  Annual Review – No changes

- 3.0 **Retired** (published on **2024-10-30**)
  Annual Review

- 2.0 **Retired** (published on **2023-11-30**)
  Annual Review - Changed Owner to Noah Webster, Chief Legal and Compliance Officer

- 1.1: **Retired** (published on **2022-12-19**)
  Changed owner to Karen Meohas. Reviewed.

- 1.0: **Retired** (published on **2022-05-17**)
  Rev 1

Approvers

- Noah Webster
- Jeremy Capell

Everbridge Data Subject Access Request Policy and Procedures

Content/Purpose

The purpose of these procedures is to establish a uniform set of instructions for responding to Data Subject Access Requests as provided for in Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and for the purpose of this document, includes the corresponding laws of the United Kingdom including the UK GDPR and Data Protection Act 2018 (collectively, the **GDPR**).

Document Information

Document Owner:	Jeremy Capell, Chief Trust Officer
Compliance Scope:	GDPR Articles 15 through 20 and 21 through Article 24(2). ISO 27701: 2019
Classification:	INTERNAL USE ONLY
Audience:	All Everbridge Employees and Contractors
Review Frequency:	Annually

TABLE OF CONTENTS

1. Purpose 5

2. Scope 5

3. Definitions 5

4. Procedures 6

4.1 Data Subject Request Submission Format 6

4.2 Tracking Data Subject Requests 6

4.3 Acknowledging Receipt of Data Subject Requests 7

4.4 Involving Relevant Departments 7

4.5 Proof of Data Subject's Identity 7

4.7 Identifying and Locating Relevant Personal Data 8

4.8 Time to Respond to Data Subject Requests 8

4.9 General Reasons for Denying a Data Subject Request 8

4.10 Fees for Responding to Data Subject Requests 9

4.11 General Rules for Responding to Personal Data Access Requests: 9

4.12 Responding to Correction (Rectification) Requests 10

4.13 Responding to Erasure Requests 10

4.14 Responding to Requests to Restrict Personal Data Processing 11

4.15 Responding to Data Portability Requests 11

4.16 Responding to Objections to Personal Data Processing 12

4.17 Responding to Automated Decision-Making Objections 13

5. Training and Awareness 13

6. Enforcement 13

1. Purpose

The GDPR grants data subjects in the European Economic Area (EEA) certain rights relating to their personal data and imposes obligations on controllers when responding to data subject requests. Everbridge has adopted this policy to address procedures for handling data subject requests and objections under the GDPR when we act as a controller.

The GDPR grants data subjects certain rights regarding their personal data including the right to:

- Access their personal data;
- Correct their personal data;
- Erase their personal data;
- Restrict personal data processing;
- Receive a copy of certain personal data or transfer that personal data to another controller, also known as data portability;
- Object to personal data processing; and
- Not be subject to automated decision-making, including profiling, in certain circumstances.

The procedures will assist Everbridge by:

- Confirming the identity of the data subject or the identity and legal authority of a third party making a request on a data subject's behalf;
- Recording and tracking data subject requests and responses, including all correspondence and internal documents related to requests;
- Reasonably Identifying and locating relevant personal data;
- Determining whether a GDPR or national law exemption exists that permits or requires us to refuse to fulfill the request;
- Handling data subject requests that involve several data subjects' personal data; and
- Communicating with data subjects at reasonable intervals regarding the status of their request.

2. Scope

This policy applies to all Everbridge employees and contractors.

3. Definitions

This policy uses the following terms:

(a) **Controller** means Everbridge, Inc. on behalf of itself and all wholly-owned subsidiaries (individually and collectively referred to as "Everbridge").
(b) **Data subject** means the person about whom the controller collects and processes personal data.
(c) **Data Subject Access Request ("DSAR")** means a written or oral request made to a controller to provide information concerning the collection and processing of a data subject's personal data.
(d) **Processor** means a natural or legal person that processes personal data (defined below) on behalf of a controller such as Everbridge's third-party vendors and sometimes, wholly-owned subsidiaries that are providing services.
(e) **Personal data** means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number, or online identifier.
(f) **Processing** means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, use, storage, dissemination, and destruction.

4. Procedures

4.1 Data Subject Request Submission Format

The GDPR does not require data subjects to submit requests in writing or use standard forms. However, Everbridge requires that data subjects submit requests in writing or electronically for the following reasons:

- Comply with the GDPR's requirements;
- Demonstrate GDPR compliance;
- Provide consistent responses;
- Formalize and streamline internal processes and procedures.

All data subjects seeking to exercise their rights under the GDPR must submit their requests in writing via post to:

Data Subject Access Request
Everbridge, Inc.
25 Corporate Drive
Suite 400
Burlington, MA 01803 USA

or electronically via email to dsar.request@everbridge.com

If you receive an oral data subject request, then respond by providing the information in Section 4.1. If you receive a data subject access request directly via email, please reply to the sender with the following message, which you can copy/paste into your response:

I am unable to receive your data subject access request. Please send it via post or email to:

Data Subject Access Request
Everbridge, Inc.
25 Corporate Drive
Suite 400
Burlington, MA 01803 USA

or

dsar.request@everbridge.com

4.2 Tracking Data Subject Requests

All data subject requests received must be forwarded to dsar.request@everbridge.com.

3.1 Through our ticketing system, the Privacy Officer ("PO") or designee must track the following about DSARs:

Essential Information:

(a) Receipt date of data subject request;
(b) Data subject name;
(c) Requester name (if applicable);
(e) Request status (new, in progress, completed);
(f) Request format;
(g) Method(s) of identification;
(h Request type and details
(j) Interim and final response date(s);

(k) Final disposition.

4.3 Acknowledging Receipt of Data Subject Requests

The PO or designee will notify the data subject in writing that Everbridge received the DSAR and a response should be provided within thirty (30) days. This notification should be sent to the data subject using the same means that the data subject used to submit the request (i.e., if request was made via email, then acknowledging receipt should be sent via email).

4.4 Involving Relevant Departments

The Office of General Counsel and Privacy Officer or designee will coordinate the DSAR response and involve necessary departments to assist.

4.5 Proof of Data Subject's Identity

Everbridge must confirm a data subject's identity before we can respond to a data subject request.

- Data subjects must provide identification that clearly shows their name and date of birth. We will accept as proof a photocopy or a scanned image of a passport or photo identification, such as a driver's license or national identification number card.
- Everbridge must securely store this information and only use it to respond to the DSAR.
- The Office of General Counsel must delete or destroy all identification documentation after confirmation of the data subject's identity.
- If the data subject's identity cannot be established using the information provided, then Everbridge must advise the data subject in writing that we need additional information to verify their identity. This response should be sent to the data subject using the same means that the data subject used to submit the request (i.e., if request was made via email, then this response should be sent via email).
- Everbridge should make clear when communicating with data subjects that the one-month time frame to respond to a DSAR does not start until we receive a fully completed request and proof of identity.
- For Unsubscribe and relevant deletions, request timelines can be abbreviated. Everbridge can use self-authentication by verifying the email address to be unsubscribed with the email from which the request was received.

4.6 Requests Made on Data Subject's Behalf

A third party (e.g. an attorney) may make a request on a data subject's behalf. In this case, we require proof of both the data subject's and third-party's identity and evidence of the third-party's legal right to act on behalf of the data subject.

- For both the data subject and the third party, we will accept as proof a photocopy or a scanned image of a passport or photo identification, such as a driver's license or national identification number card.
- Everbridge must securely store this information and only use it to respond to the DSAR.
- The Office of General Counsel must delete or destroy all identification documentation after confirmation of identity.
- If the identity cannot be established using the information provided, then Everbridge must advise the data subject and third party in writing that we need additional information to verify their identity. This response should be sent to the data subject and third party using the same means that it was sent to Everbridge (i.e., if request was made via email, then this response should be sent via email).
- Everbridge should make clear when communicating with both parties that the one-month time frame to respond to a DSAR does not start until we receive a fully completed request and proof of identity.

4.7 Identifying and Locating Relevant Personal Data

The Privacy Officer or designee is responsible for leading the effort to locate personal data relevant to a data subject request. They must:

(a) Identify all departments that might reasonably be considered to hold personal data relevant to the request; and
(b) Work with those departments to collect the personal data about the data subject from relevant sources such as:

- emails, electronic files, documents and systems;
- databases;
- automated systems such as door entry or key card access systems;
- word processing systems;
- computer hard drives;
- hard copy files;
- voice recordings;
- photographs;
- monitoring records and CCTV images;
- internet logs;
- telephone records;
- back-up files; and
- third-party data processors' systems.

The departments identified play a key role in responding accurately to a DSAR. Each department will assign one or more staff members, as necessary, to facilitate collection of personal data from sources they can access. The assigned staff members shall be required to make reasonable efforts to find and access personal data and shall respond promptly to the Office of General Counsel and PO during the collection effort.

The Privacy Officer or designee must review the files and the documents collected and identify whether the information gathered is personal data relevant to the request.

If the scope of the DSAR is unclear or does not provide sufficient information to conduct a search (for example, the request asks for "all information about me"), then the PO or designee must notify the data subject in writing. Notification should explain why the original request is not sufficient and that a more detailed request is needed. Everbridge should make clear when communicating with the data subject that the one-month time frame to respond to a DSAR does not start until we receive information sufficient to conduct a search.

The Privacy Officer or designee must retain internal documents that show the steps and efforts made to locate relevant personal data, including all the search methods used.

4.8 Time to Respond to Data Subject Requests

The GDPR requires that a controller (like Everbridge) respond to a DSAR no later than 1 month after it's received, unless additional time is needed. If more time will be needed, then the Privacy Officer must inform the data subject within one month of receipt of the request of the extension and explain the reason(s) for the delay.

4.9 General Reasons for Denying a Data Subject Request

There are circumstances that exempt Everbridge from responding to a DSAR. The Office of General Counsel will make the determination about whether one or more of the following exemptions apply:

(a) A third party fails to present sufficient proof of authority to make the request on the data subject's behalf.

(b) When we process data for purposes that do not require data subject identification and we demonstrate that we cannot identify the data subject, we may deny data subject requests unless the data subject provides additional information enabling identification.
(c) National law provides a basis for denying the request.
(d) We demonstrate that the request is manifestly unfounded or excessive, in particular because of its repetitive character.
(e) We do not hold any personal data related to the data subject request.

If we do not have or process personal data related to the data subject, then the Privacy Officer should indicate that we conducted a diligent search for records related to the data subject's request and did not uncover responsive results. The Privacy Officer should retain internal documents that show the steps we took to locate relevant personal data, including all the search methods used.

In the event that we are not the data controller for the requested information, the request will be denied. The requester will be informed of our status and advised to contact the relevant data controller.

4.10 Fees for Responding to Data Subject Requests

A DSAR is generally provided free of charge. However, Everbridge is entitled to charge a fee when requests are manifestly unfounded or excessive, because of their repetitive character or when the request relates to large amounts of data. The Office of General Counsel will make the determination about whether to charge fees. The Privacy Officer must document the reasons for charging fees.

4.11 General Rules for Responding to Personal Data Access Requests:

Data subjects have the right to request access to their personal data processed by us under Article 15 of the GDPR.

Unless an exemption applies and based on the relevant scope, the Privacy Officer or designee must provide data subjects with the following information about Everbridge's personal data processing activities:

- The purposes of processing;
- Categories of personal data processed;
- Recipients or categories of recipients who receive personal data from us;
- How long we store the personal data or the criteria we use to determine retention periods;
- Information on the personal data's source if we do not collect it directly from the data subject;
- Information on the safeguards we use to secure transfers of personal data to non-EU countries or to an international organization;
- Whether we use automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing;
- Their right to:
    - request correction or erasure of their personal data;
    - restrict or object to certain types of processing with respect to their personal data; and
    - make a complaint with the local data protection authority.

The Privacy Officer or designee must provide the data subject with a copy of the personal data we process about the data subject in a commonly used electronic form, unless an exemption applies, like:

Personal Data Pertaining to Third Parties:

(a) In certain cases, we process personal data that contains the personal data of several data subjects. The data subject access right must not adversely affect the rights and freedoms of third parties.

(b) Where the data set includes third-parties' personal data, we must identify a legal basis under the GDPR prior to transferring the third-parties' data. The Office of General Counsel must determine whether we have a basis to transfer the third-party's data.
(c) In cases where the Office of General Counsel determines that we do not have a basis to transfer the personal data of third parties, the Privacy Officer or designee may give instructions to redact or remove the personal data of the third parties prior to providing the data in response to an access request.

In addition, we may also refuse to respond to a data subject request if the data subject requests a copy of the personal data we process and providing a copy is likely to adversely affect the rights and freedoms of others. The Office of General Counsel must determine if we have a basis not to respond to a data subject access request. The Privacy Officer or designee must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

4.12 Responding to Correction (Rectification) Requests

Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data.

The Privacy Officer or designee must identify each third-party recipient of the personal data that is the subject of the rectification request and communicate the rectification of the personal data to each recipient (for example, our third-party service providers who process the data on our behalf), unless the Office of General Counsel issues a written finding that it is impossible or involves disproportionate effort. The Privacy Officer or designee must also inform the data subject about those recipients if the data subject requests it.

4.13 Responding to Erasure Requests

Data subjects have the right to have us erase their personal data.

The Privacy Officer or designee must erase the personal data that is the subject of the request if:

- The personal data is no longer necessary for the purpose we collected it for;
- The data subject withdrew his or her consent to our processing activities and no other legal justification for processing applies; or
- The data subject objects under certain sections of the GDPR.

If we determine that we must erase the data subject's data in response to the request, then the Privacy Officer or designee must identify each recipient to whom we disclosed that personal data. The Privacy Officer or designee must communicate the erasure of personal data to the third-party data recipients, unless the Office General Counsel legal issues a written finding that this is impossible or involves disproportionate effort.

In addition to the general grounds for denying a data subject request set out above, we may also refuse to respond to a data subject erasure request if we process personal data that is necessary for:

- Exercising the right of freedom of expression and information;
- Complying with a legal obligation under EU or member state law;
- The performance of a task carried out in the public interest;
- Exercising our official authority;
- Public health reasons consistent with the exceptions for processing sensitive personal data such as health information, as outlined in GDPR Articles 9(2)(h) and (i) and 9(3);
- Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1), if the erasure is likely to render impossible or seriously impair the processing objectives; or
- The establishment, exercise, or defense of legal claims.

The Office of General Counsel must determine if we have a basis not to respond to a data subject erasure request. The PO or designed must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

4.14 Responding to Requests to Restrict Personal Data Processing

Data subjects have the right to request that we restrict the processing of their personal data.

The Privacy Officer must restrict processing if:

- The data subject contests the accuracy of the personal data. We must restrict processing the contested data until we can verify its accuracy;
- The processing is unlawful. Instead of requesting erasure of the data, the data subject can request that we restrict use of the unlawfully processed personal data;
- We no longer need to process the personal data but the data subject needs the personal data for the establishment, exercise, or defense of legal claims;
- A data subject objects to processing, including profiling, for:

    - purposes that we consider necessary to perform a task in the public interest; or
    - purposes that we consider necessary for our or a third party's legitimate interests.

The Office of General Counsel must determine if we have a basis not to respond to the data processing restriction request. The Privacy Officer or designee must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

Where processing has been restricted, the Privacy Officer must ensure that we only process the personal data (excluding storing it) either:

a) With the data subject's consent;
b) For the establishment, exercise, or defense of legal claims;
c) For the protection of the rights of another person;
d) For reasons of important public interest;

The Privacy Officer or designee must inform the data subject that we intend to lift the restriction 14 days before lifting the restriction. We may lift the processing restriction when:

- the Privacy Officer verifies the accuracy of the personal data that is the subject of the processing restriction request; or
- the Office of General Counsel determines that our or a third-party's legitimate interests override the data subject's interests;.

Where processing has been restricted, the Privacy Officer or designee must identify each recipient to whom we disclosed the personal data to inform them of the processing restriction to the unless the Office of General Counsel issues a written finding that it is impossible or involves disproportionate effort.

4.15 Responding to Data Portability Requests

Data subjects have the right to:

- Receive a copy of certain personal data from us in a structured, commonly used, and machine-readable format and store it for further personal use on a private device;
- Transmit certain personal data to another controller;
- Have us transmit certain personal data directly to another controller, where technically possible.

The data portability right only applies to personal data processed by automated means when processing is either:

a) Based on the data subject's consent; or
b) Necessary to perform a contract with the data subject.

The personal data covered by the data portability right includes only personal data concerning the data subject which the data subject knowingly and actively provided to Everbridge such as name, contact information, and browsing history.

The data portability right does not include data that we create from the data provided by the data subject such as a user profile. If you have any questions about whether personal data falls within the scope of a data subject portability request, please contact the Privacy Officer.

For personal data that the data subject requests be transmitted to a third party, the Privacy Officer or designee must transfer that personal data by electronic means. If the data subject asks that the information be provided to them directly, Privacy Officer or designee must transfer that personal data by electronic means.

4.16 Responding to Objections to Personal Data Processing

Data subjects have the right to object to personal data processing when we process their personal data:

- For direct marketing purposes, including profiling related to direct marketing. We must stop processing a data subject's personal data for direct marketing purposes whenever the data subject objects; and
- For scientific or historical research purposes or statistical purposes, subject to certain exceptions.

The Privacy Officer or designee must stop the personal data processing related to the data subject's request.

Everbridge can refuse to grant a data subject processing objection when:

- A data subject objects to processing for scientific or historical research purposes or statistical purposes and we demonstrate that the processing is necessary for us to perform a task in the public interest;
- A data subject objects to processing, including profiling, based on Articles 6(1)(e) (processing for a task carried out in the public interest or the exercise of official authority vested in us) or 6(1)(f) (processing necessary for the legitimate interests of us or a third party) and we demonstrate:

    - a compelling legitimate ground for processing the personal data that overrides the data subject's interests; or
    - that we need to process the personal data to establish, exercise, or defend legal claims.

If the Office of General Counsel determines that there are no overriding legitimate grounds for the personal data processing then the Privacy Officer or designed must erase that personal data.

The Office of General Counsel must determine if we have a basis not to respond to a data subject's objection request. The Privacy Officer or designee must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

4.17 Responding to Automated Decision-Making Objections

Data subjects have the right not to be subject to a decision based solely on the automated processing of their personal data, including profiling, if the decision produces legal or other similarly significant effects on them. The Office of General Counsel must determine if the automated decision-making, including profiling, produces legal effects on the data subject or affects them in a similarly significant way.

The Privacy Officer or designee must stop the automated decision-making that is the subject of the request.

Everbridge can refuse to grant an automated decision-making objection when the automated decision is either:

(a) Necessary for entering into or performing a contract with the data subject;
(b) Authorized by EU or member state law applicable to us; or
(c) Based on the data subject's explicit consent.

The Office of General Counsel must determine if we have a basis not to respond to the data subject's automated decision-making objection. The Privacy Officer or designee must inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

5. Training and Awareness

This procedure will be published on Everbridge's website. The Privacy Officer must ensure that all staff subject to the policy understand their roles in implementing through training, communications, and team meetings.

6. Enforcement

Violations of this policy may result in disciplinary action, in accordance with Everbridge's information security policies and procedures and human resources policies.