Privacy & Security | GENERAL DATA PROTECTION REGULATION (GDPR)

DATA SUBJECT REQUESTS UNDER THE GDPR: A STEP BY STEP GUIDE

BEFORE YOU RECEIVE A REQUEST

1. Determine whether you are subject to the General Data Protection Regulation (GDPR) and whether you are acting as a "data controller" or "data processor." A controller directs how data is used, and a processor carries out the controller's directions. Controllers are required to fulfill data subject requests; however, processors may be obligated to assist controllers in fulfilling these requests.

2. Conduct a data mapping exercise to understand what personal data your company collects (including from customers, vendors, and employees), how it is used and shared, and where it is stored by the company and any third parties (e.g., service providers that process the data on the company's behalf).

3. Establish a preferred method of receiving and escalating data subject requests from employees, customers, and vendors (e.g., this may include an online web form, an internal email address, a customer portal, etc.). Privacy policies and notices should also be updated to direct data subjects to use the preferred channels. Employees who are likely to interact with data subjects and receive such requests directly should receive training so that they know how to reroute data subject requests to the appropriate channel(s).

4. Create or review internal policies and procedures for responding to data subject requests to access, correct, and erase data, restrict data processing, transfer data, and object to certain data processing. The policies should indicate who handles these requests and the schedule for receiving, evaluating, responding to, and fulfilling requests. The procedures should include a system for keeping records of data processing, a means of filtering data to easily identify the data for which the person is making the request, template responses to requests, and a method for transferring data electronically.

5. Review systems, applications, processes, and technical controls that might be relevant to supporting a data subject request. If personal data resides across many systems within the organization, it may be worth checking to determine the most optimal location to interact with the data (whether accessing it, correcting it, transferring it, restricting its use, or erasing it). It is also a good idea to ensure that the data in the system/application/location chosen to service these requests contains accurate data before disclosing.

6. Inform data subjects of their rights under the GDPR (e.g., by updating privacy policies) and how they can exercise those rights.

ONCE YOU RECEIVE A REQUEST

1. Identify the person making the request. If you cannot identify the person making the request, you do not have to fulfill the request; however, you must be able to show that you are not in a position to identify the person. You are not required to obtain further information from the person in order to connect the person to his or her data.

2. Acknowledge receipt of the request and ask for additional information that may be necessary.

3. Determine whether a restriction applies, such that you should deny the request or otherwise limit fulfillment of the request. (Refer to the chart at the end for a list of possible restrictions.)
4. Decide whether you need more information to fulfill the request.

WHEN RESPONDING TO A REQUEST

1. Keep in mind that you cannot charge a fee to fulfill a request unless the request is manifestly unfounded or excessive.
2. Acknowledge receipt and request additional information (if necessary) from the person to fulfill the request. Make sure to fulfill the request within a month of receipt. If you must deny the request, notify the person without delay and not later than one month after receiving the request. If you need more time to fulfill the request, a two-month extension is allowed as long as this is communicated to the person. Inform data subjects of their rights under the GDPR (e.g., by updating privacy policies) and how they can exercise those rights.
3. Consider whether additional steps should be taken to protect other people's rights. For example, for access requests, you should filter and/or redact data, as necessary, to protect other people's privacy.
4. Consider whether additional details must be included in your response. For example, responses to access requests must include the following information in addition to access to the data:
    - the purposes of the processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations, and any safeguards for the transfer of this data;
    - the period for which the data will be stored;
    - the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the person or to object to such processing;
    - the right to lodge a complaint with a supervisory authority;
    - the source of the data (if not collected from the data subject); and
    - the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
5. Fulfill the request. If the person has requested access to her or his data, provide a copy of the personal data undergoing processing. This should be provided in a commonly used electronic form if the person has submitted the request electronically.
6. Record the company's fulfillment of the request. This record can include, for example, details on what the request was for, who made the request, when the request was made, and when the request was fulfilled. This will help flag duplicate/excessive requests indicating that denying, or charging a fee for, a future request may be warranted.

Possible restrictions requiring denial or limited fulfillment of data subject requests.	
ACCESS (ART. 15)	· The request is manifestly unfounded or excessive. (Burden is on controller to show this.) · Controller is subject to a Member State or Union law that restricts its ability to fulfill the request. · Providing copy of data would adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. (This requires appropriately scoping the fulfillment of the request—through redaction, etc.—not denying the request altogether.)
CORRECT (ART. 16)	· The request is manifestly unfounded or excessive. (Burden is on controller to show this.) · Controller is subject to a Member State or Union law that restricts its ability to fulfill the request.
ERASE (ART. 17)	· The request is manifestly unfounded or excessive. (Burden is on controller to show this.) · Controller is subject to a Member State or Union law that restricts its ability to fulfill the request. · Keeping data is necessary for freedom of expression or freedom of information. · Keeping data is necessary for compliance with a legal obligation that requires processing by Union or Member State law to which controller is subject. · Keeping data is necessary for performing a task for the public interest or in the exercise of official authority vested in controller's company. · Keeping data is necessary for public interest reasons related to public health. · Keeping data is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes, if erasure is likely to seriously impair or make impossible the objectives of this work. · Keeping data is necessary for establishing, exercising or defending legal claims.
RESTRICT (ART. 18)	· The request is manifestly unfounded or excessive. (Burden is on controller to show this.) · Where processing has been restricted, personal data may be processed for the establishment, exercise or defense of legal claims. · Where processing has been restricted, personal data may be processed for the protection of the rights of another natural or legal person. · Where processing has been restricted, personal data may be processed for reasons of important public interest of the Union or of a Member State. · Controller is subject to a Member State or Union law that restricts its ability to fulfill the request.
TRANSFER (ART. 20)	· The legal basis of processing is not based on consent or on performance of a contract. · The request is manifestly unfounded or excessive. (Burden is on controller to show this.) · Controller is subject to a Member State or Union law that restricts its ability to fulfill the request. · Providing copy of data would adversely affect the rights and freedoms of others. (This requires appropriately scoping the fulfillment of the request—through redaction, etc.—not denying the request altogether.)

OBJECT (ART. 21)	• The request is manifestly unfounded or excessive. (Burden is on controller to show this.) • Controller is subject to a Member State or Union law that restricts its ability to fulfill the request. • The controller has compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject. • The processing is for the establishment, exercise, or defense of legal claims. • The processing is necessary for performance of a task carried out in the public interest (where the processing is for scientific or historical research or statistical purposes).