

GDPR – Data Subject Policy & Procedure

Vendasta Technologies Inc.

Last modified: February 8, 2023

PART 1: Data Subject Rights

Within the meaning of GDPR, "Personal data" means any information relating to an identified or identifiable natural person ("data subject"). GDPR grants data subjects a range of specific data subject rights they can exercise, with exceptions. Data subject requests are not new, but GDPR introduced some changes to further protect their rights.

Under Article 12(2) of the GDPR, we are obliged to comply with a DSR without undue delay and, in any event, within one month (i.e. a calendar month) of receiving a request from a data subject or their representative after establishing its identity. Any refusal of a DSR must also meet this timescale. Taking account of the complexity and number of requests made by the data subject, the period for responding may be extended by a further period of two months. Data subject must be informed of any extension or refusal, with reasons, within one month of receipt of the request. Failure to respond to DSRs can leave organizations open to the higher level of administrative fines under the GDPR: €20 million or up to 4% of annual global turnover – whichever is greater.

General Points Applicable to All DSRs

- Data subjects can make a request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact. It does not have to include the title 'request for rectification' or 'request to Erasure' etc or mention Article number of the GDPR, as long as it is clear that the data subject is making a request about its own personal data.
- We have a legal responsibility to identify the data subject (if a representative is acting on behalf of the data subject then we have a legal responsibility to verify its authorisation as well) who has made a request and also to check the information requested falls in the personal data category to validate the request.
- We must comply with a validated request within a month, if it needs a lot of effort then it can be extended to two more months but about this extension and the reason must be informed to the data subject within a month from validating the request.
- If any exemption applies to a request we can refuse to comply with it. Also, manifestly unfounded or excessive requests can either be refused or charged a "reasonable fee" for the administrative costs.
- In all cases when we refuse to comply or charge for administrative fee or ask for more information for identification, we have to inform the data subject within a month: the reasons we are not taking action or charging the request; their right to make a complaint to the ICO or other authorities; and their ability to seek to enforce this right through a judicial remedy.
- It is good practice to keep record of all the details of the request and log the process details, this can help avoid later disputes if any, about how we have interpreted and processed the request to be in compliance.

Right to be Informed

At the point where personal data is collected from the data subject (Article 13) or obtained from another source (Article 14), there is a requirement to inform the data subject about our use of their personal data and their rights over it to ensure transparency. Compliance with this right is addressed in a separate document, Privacy policy, which describes our identity,

contact information, the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries or sharing with third parties, how we will process and safeguard their personal data. Also, inform the data subject about the duration of storage, their rights, the ability to withdraw consent, the right to lodge a complaint with the authorities. In addition, the data subject must be informed of any automated decision-making activities, including profiling.

Right to Withdraw Consent

The data subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (i.e. the processing is not based on a different justification such as contractual or legal obligation). Before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the basis of the processing. If not, then the request may be rejected. In many cases, the giving and withdrawal of consent will be available electronically i.e. online and doesn't need separate procedure. Note – Where consent involves a child (age 18 or under) the giving or withdrawal must be authorised by the holder of parental responsibility over the child.

Right of Access

A data subject has the right to obtain confirmation from us if we are processing their personal data (Article 15) and to access that personal data and supplementary information, to understand how and why we are using their data, and check if we are doing it lawfully.

Right to Rectification

Personal data is considered inaccurate if it is incorrect or misleading as to any matter of fact. A data subject has the right to have inaccurate personal data rectified and also be able to have incomplete personal data completed depending on the purpose for the processing (Article 16). We should take reasonable steps to make sure that the data is accurate and to rectify the data if necessary, taking into account the arguments and evidence provided by the data subject especially if it is used to make significant decisions that will affect a data subject or others. Where possible, and where it would not involve disproportionate effort, any third party with whom rectified data have been shared should be informed of the rectification.

Right to Erasure

Also known as "the right to be forgotten" (Article 17), the data subject has the right to require us to erase personal data about them without undue delay where one of the following applies:

- The personal data are no longer necessary for the purpose for which they were collected
- The data subject withdraws consent and there is no other legal ground for processing
- The data subject objects to the processing of the personal data
- The personal data have been unlawfully processed

- For compliance reasons, i.e. where it needs to be removed to meet the legal obligations by us
- Where the personal data was relevant to the data subject as a child

Reasonable efforts must be made to ensure erasure where the personal data has been made public.

Right to Restriction of Processing

The data subject has right to a restriction of processing of their personal data in one of the following circumstances (Article 18):

- Where the data subject contests the accuracy of the data, until we have been able to verify its accuracy
- As an alternative to erasure in the circumstances that the processing is unlawful
- Where the data subject needs the data for legal claims but it is no longer required by us
- Whilst a decision on an objection to processing is pending

Where a restriction of processing is in place, the data may be stored but not processed without the data subject's consent, unless for legal reasons (in which case the data subject must be informed). Third parties who may process the data on our behalf must also be informed of the restriction.

Notification Obligation

If we have shared and/or disclosed personal data with the third parties, we are required to communicate (Article 19) any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17 and Article 18 to each recipient, unless this proves impossible or involves disproportionate effort. Also, we need to inform the data subject about these third parties with whom we have shared their personal data, if the data subject requests it.

Right to Data Portability

The data subject has the right to request that their personal data be provided to them in a "structured, commonly-used and machine-readable format" (Article 20) and/or to transfer their personal data to another party e.g. service provider where technically feasible without any hindrance. This applies to personal data provided by the data subject in a machine readable format for which processing is based on the data subject's consent or on a contract and the processing carried out by automated means.

Right to Object

A data subject (Article 21) has the absolute right to object to the processing of their personal data if it is for direct marketing purposes. The right to object is limited if their data is processed for scientific or historical research, or statistical purposes. The right to object is not absolute if the processing is for:

- a task carried out in the public interest;

- the exercise of official authority vested; or
- legitimate interests (or those of a third party).

Where the data are being processed for a law enforcement purpose, there is no right to object.

Right to Automated Decision Making and Profiling

The data subject has the right to not be the subject of automated decision-making including profiling where the decision has a significant effect on them, and they can insist on human intervention where appropriate (Article 22). The data subject also has the right to express their point of view and contest automated decisions. There are exceptions to this right, which are if the decision:

- Is necessary for a contract
- Is authorized by law
- Is based on the data subject's explicit consent

Other Communication – Personal Data Breach Notice

We have a duty to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting data subjects' rights and freedoms, we must also inform those data subjects without undue delay.

PART 2: Data Subject Rights Request Procedure

Last modified: January 13, 2022. This page is regularly updated to reflect continued monitoring, accuracy and comprehensiveness.

SECTION ONE – Introduction

Within the meaning of GDPR, "Personal data" means any information relating to an identified or identifiable natural person ("data subject"). GDPR grants data subjects a range of specific data subject rights they can exercise, with exceptions. Data subject requests are not new, but GDPR introduced some changes to further protect their rights. GDPR compliance among others means enabling the exercise of these rights. Failure to respond to DSRs can leave organizations open to the higher level of administrative fines under the GDPR: €20 million or up to 4% of annual global turnover – whichever is greater.

SECTION TWO – Data Subject Rights

The right to be informed, The right of access, The right to rectification, The right to erasure, The right to restrict processing, The right to data portability, The right to object, Rights in relation to automated decision making and profiling.

SECTION THREE – What is a Data Subject Rights Request?

Data Subject Rights (DSRs) request is a request about (and identifying) a living person, made by that person or by a third party with appropriate authority acting on behalf of the person to exercise their rights, governed by Article 15 of the GDPR.

Under Article 12(2) of the GDPR, comply with a DSR without undue delay and, in any event, within one month (i.e. a calendar month) of receiving a request from a data subject or their representative. Any refusal of a DSR must also meet this timescale. Taking account of the complexity and number of requests made by the data subject, the period for responding may be extended by a further period of two months. Data subject must be informed of any extension, with reasons, within one month of receipt of the request.

SECTION FOUR – Data Subject Rights Request Handling Procedure

DS Requests under GDPR apply to personal data/information/files/records relating to data subjects. The following general points apply to all of the requests described in this document and are based on Article 12 of the GDPR:

1. We have to provide requested Information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

2. Data subjects can make a request verbally or in writing. It can also be made to any part of Vendasta (including by social media) and does not have to be to a specific person or contact. It does not have to include the title of the request formally or mention Article number of the GDPR, as long as it is clear that the data subject is making a request about its own personal data.

3. We have a legal responsibility to identify data subject (if a representative is acting on behalf of data subject then we have a legal responsibility to verify its authorization as well). In case of doubt about identity, we may request further information to establish it.

4. We must act on a request from a data subject, unless we are unable to establish their identity. (a) We must provide information without undue delay and within a maximum of one month from the receipt of the request. (b) The response timescale may be extended by up to two further months for complex or a high volume of requests – the data subject must be informed of this within one month of the request, and the reasons for the delay given.

5. If a request is made via electronic form, the response should be via electronic means where possible, unless the data subject requests otherwise.

6. If it is decided that we will not comply with a request, we must inform the data subject without delay and at the latest within a month, stating the reason(s) and informing the data subject of their right to complain to the supervisory authority.

7. Generally, responses to requests will be made free of charge, unless they are “manifestly unfounded or excessive” (Article 12 of the GDPR), in which case we will either charge a reasonable fee or refuse to action the request but the data subject must be informed of this within one month of the request, with the reasons.

Important to Note: Pursuant to Article 29, the GDPR simply states to use “all reasonable measures” to verify the identity of requestor and ensure to not disclose personal data to the wrong person, infringe any data subject rights, or make it too difficult for the data subjects to exercise their rights, any of which would violate the GDPR.

SECTION FIVE – Data Subject Rights Request Procedural Flowchart

The procedure for responding to requests from data subjects is set out in a flowchart. The specifics of each step in the procedure may vary according to the type of request involved. For the full procedural flowchart, please refer to the online version at trust.vendasta.com.

SECTION SIX – Summary of Data Subject Rights by Lawful Basis of Processing

The following table shows which rights of the data subject are relevant to each basis of lawful processing. It should be used as a general guide only, as the specific circumstances may affect the validity of the request.

Note: All of the above assume that: 1. the personal data are being lawfully processed; 2. The personal data are necessary in relation to the purposes for which they were collected or otherwise processed. If this is not the case, then further investigation must be made regarding the validity of the request.