Newable

Subject Access Request Policy (under GDPR)

Version 1.0

July 2021

© 2021 Newable

Newable

Version Control

Version	Owner	Reviewer	Changes	Approval date	Next Review
1.0	Joanne Wilkinson	Michael Walsh	Initial version or first version uploaded on portal - see ESG share for historical information	07/2021	03/2022

© 2021 Newable

Newable

Purpose

This policy seeks to ensure that Newable processes a Subject Access Request (“SAR”), from a data subject (including clients and employees), or designated third party, in accordance with the General Data Protection Regulation (GDPR).

© 2021 Newable

Newable

Scope

This policy applies to:

1. All Newable employees, temporary staff, contractors, and third parties as related to the authorised use of Newable information, customer/client information and information covered under a Non-Disclosure Agreement (NDA).
2. Any individual who wishes to access a copy of the personal data any Newable business unit holds about them and they are entitled to be:
    i. told whether any of their personal data is being processed;
    ii. given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
    iii. given a copy of the personal data; and,
    iv. given details of the source of the data (where this is available).

This policy does not apply to information that is requested in the course of normal business (i.e., sending a copy of a statement or letter or interview feedback etc.)

© 2021 Newable

Newable

Policy

Definitions

Subject Access Request (SAR)

A written request made by an individual to Newable to supply them with a copy of all personal information that is held about them, which includes electronic and paper based records. The entitlement to ask for information is covered under the GDPR.

Data Subject

The individual to which the particular personal data relates.

Data Controller

Newable Group

Third Party Request

Often a solicitor acting on behalf of an individual. It could also be someone with a Power of Attorney which allows them to act on behalf of another individual.

Responsibilities

Data Protection Officer (DPO)

Joanne Wilkinson, Head of Compliance and Money Laundering Reporting Officer is also the DPO who is responsible for ensuring that all SARs are handled in an effective, professional and timely manner. Additionally, the DPO has the responsibility for ensuring that all SARs are logged and the log maintained for an appropriate length of time in order to handle standard SARs, abandoned SARs and any investigations by the UK Information Commissioner's Office (ICO).

Employees, temporary staff and contractors

All employees, temporary staff and contractors must supply the DPO, on request and in a timely manner, with all personal data related to the data subject, in response to the SAR. If any staff become aware of a SAR, they should notify the DPO immediately.

Procedure

The following procedure should be followed when responding to a SAR:

© 2021 Newable

Newable

Receive the request

1. The Data Subject may request access to their data via any employee, temporary staff or contractor at any of the Newable offices or the request may be made directly to the DPO.
2. A request must be made in writing. A request sent by email or fax is as valid as one sent in hard copy. Requests may also be considered valid through social media.
3. If the request is made verbally, there is no obligation to respond. However, it is good practice to at least explain to the individual how to make a valid written request, rather than ignore them.
4. Any permanent or temporary employee or contractor receiving such a request, must ensure that the request is *immediately* forwarded to the Newable DPO.
5. The DPO must provide the Data Subject with the information requested without delay, and at the latest within one month of receipt of the request. The information must usually, be provided free of charge.
6. Many organisations require individuals to use a SAR Form. However, there is no compulsory requirement for an individual to complete the form and this must not be used as a means of extending the one month timeframe for responding. Any request in writing must be considered a valid request, irrespective of the format.

Verify the request

1. If a SAR Form is used to obtain information from the individual, it should be checked to verify that it has been completed correctly and that all information relevant for the request has been obtained.
2. If the form, or original request from the individual, does not contain all the necessary information to process the request, a letter requesting additional information (along with the original form where relevant) must be sent to the applicant. Details of the request should be recorded in the subject access request log.
3. In instances where a SAR is made on behalf of the data subject, either by another individual or through a solicitor, then written authorisation must be obtained from the data subject. This authorisation must be verified and identification of the data subject must be obtained.

Log the request

1. If the request has been received before (i.e. returned to the data subject for additional information) then the subject access request log should be updated to reflect this.
2. If the request is new, and contains all the information required to validate the data subject's identity, then it should be recorded in the SAR log.
3.

© 2021 Newable

The subject access request log should contain the following details:

i. A unique reference number for any future internal or external correspondence;
ii. A status of active or closed;
iii. The date the SAR was received;
iv. Name, address and date of birth of the data subject;
v. An indication as to what proof of ID was provided to verify the identity of the data subject – e.g. passport and recent utility bill;
vi. An indication as to the type of data that needs to be searched – i.e. client records, employee records, CCTV, archived paper records, email, network drives etc.;
vii. The date that a request was sent to the Newable business unit(s) to begin the search for the data subject's records as well as the names to which the request was sent;
viii. The date that a request was received back from the Newable business unit with the search results;
ix. The date by which the SAR needs to be fulfilled (i.e. within one month from receipt of and the information to validate the data subject's identity is received); and,
x. Any other relevant comments.

4. When a valid request has been received (i.e. the information to validate the data subject's identity), then a letter of acknowledgement must be sent to the data subject, or their representative.

Process the request

1. Initiating the Search
    i. The DPO will email the request details to the relevant Newable business units who are responsible for the data and will advise the business unit of:
        a. the date the SAR was received;
        b. the date by which the search needs to be completed; and,
        c. the information required to support the search.
    ii. Any questions or anticipated delays in responding to the search must be communicated to the DPO immediately.
2. Performing the Search
    i. The Newable business unit will search for the data in applicable systems, paper records, email, CCTV and network drives etc.
    ii. The details of the data subject will be presented in a suitable, easy to understand format. An explanation of any codes or references must be provided.
    iii. No information must be sent to the data subject that enables the data subject to identify a third party individual, unless express permission has been sought from that third party individual.
    iv. Care must be taken to ensure that the identity of a third party individual is not

© 2021 Newable

inadvertently disclosed by either redacting their personal data or by providing the information in another format.

v. Information held for the prevention and detection of a crime (e.g. a current fraud investigation or litigation) does not need to be disclosed. However, once the investigation has been completed, then the information must be released if a data subject requests access to their data.
vi. A copy of all the data retrieved must be logged in the SAR log for reference, just in case the data subject challenges the data.
vii. If no data can be found, then the Newable business unit must inform the DPO.

3. Providing Data
    i. Handling Negative Search Results
        a. *No data:* The DPO will respond to the data subject, or their representative, stating that no personal data was found, the search parameters used and any reasons, if appropriate, as to why the data was not found (e.g. potentially data disposed of in line with legal retention requirements).
        b. *Exemptions:* If any exemptions exist as to why the data cannot be provided then this must be communicated to the data subject.
    ii. Handling Positive Search Results
        - Depending on the amount and type of data, it may be easier to provide it in printed format, via post, or electronically, via email.
        - In most cases, the data should be provided in hard copy format. However, if the data subject, or their representative, has indicated a preference, then Newable will comply with this preference.
        - The data must be in a format that will be understood by the data subject with an explanation of any codes that have been used.
        - The information must be provided to the applicant within one month of receiving a valid request (i.e. receipt of verification of identity documents to process the request).
        - Data sent out via post must be appropriately sealed and sent out via secure and recorded delivery.
        - Data sent via email must be encrypted.

Charging a fee for a SAR

The ICO Guidance states that in most cases a firm cannot charge a fee for a SAR, however, where the request is manifestly unfounded or excessive, a firm may charge a “reasonable fee” for the administrative costs.

In cases where Newable deems it appropriate to charge a fee, the rationale for charging the fee and the basis of calculation should be included on the SAR log by the DPO. A guideline fee of £25 per hour would be reasonable.

© 2021 Newable

Newable

A SAR deemed to be manifestly unfounded or excessive

A SAR request may be considered to be “manifestly unfounded or excessive” in the following circumstances:

1. If the request could fairly be seen as obsessive
2. If the request harasses the organisation or causes distress to staff
3. If complying with the request imposes a significant burden in terms of expense and distraction
4. If the request is designed to cause disruption or annoyance
5. If the request lacks any serious purpose or value

The DPO is responsible for assessing whether a request could be considered “repeated, voluminous or vexatious”, and if it is, then the DPO must record the rationale on the SAR log.

The process for refusing a request

A SAR request can be refused in the following circumstances:

1. It would cost too much or take too much staff time to deal with the request
2. The request is vexatious
3. The request repeats a previous request from the same person

If the DPO decides to refuse all or any part of a request, then the DPO must send the data subject a written refusal notice. The DPO can issue a refusal notice in the following circumstances:

1. If the DPO refuses to say whether Newable holds the information at all
2. Where the DPO confirms that the information is held, however, Newable refuses to release it

In the instance that the DPO decides to refuse a SAR request, then the rationale must be included on the SAR log and in the response to the data subject.

Closing the request

When all details have been passed to the data subject, or their representative, then the SAR log must be updated accordingly, including the type of data that was sent out and when it was sent.

30 days after the data has been sent out, the status of the SAR can be changed to “closed”. All details and data relevant to the subject access request, whether or not data was provided, should be retained for two years.

© 2021 Newable

Newable

Appeals

If the data subject is not satisfied with the response, then they should contact the DPO who will consider the request and deal with it accordingly.

The DPO should encourage the data subject to attend a meeting to resolve any concerns.

© 2021 Newable