WealthWizards

Data Protection - Data Subject Access Request (DSAR) Process

Version 11 (06 March 2023)

Introduction

The General Data Protection Regulation (GDPR) expands the rights of individuals to control how their personal information is collected and processed, and places obligations on Wealth Wizards to be more accountable for the management of personal data.

Article 15 of Section 2 of the GDPR – Right of access by the Data Subject

The Data Subject shall have the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the Data Subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.
- Where personal data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

Article 12(5) of the GDPR states that information shall be provided, and actions taken in relation to an access request, free of charge. However, the article says:

"where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may either:

- *Charge a reasonable fee taking into account the administrative costs for providing the information or communication or taking the action requested; or*
- *Refuse to act on the request.*

The Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request".

In addition, Article 15(3) of the GDPR states:

“The Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the Data Subject, the Controller may charge a reasonable fee based on administrative costs.”

Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Definitions

GDPR	The UK General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the UK.
Data Subject	The Data Subject is the individual whom particular personal data is about. The Act does not count as a Data Subject an individual who has died or who cannot be identified or distinguished from others.
Data Controller	The Data Controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	The Data Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Personal Data	Personal Data is defined as any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Procedure

- Identify the request.
- Log and report internally.
- Check formalities.
- Check identity and authority.

- Acknowledge receipt and request further information.
- Diarise deadline.
- Leave enough time to locate data and prepare response.
- Set search parameters and undertake search.
- Data exclusions? (e.g. third-party data or exemptions).
- Prepare copies ready for disclosure.
- Prepare other information (e.g. purposes, recipients, sources, explanations).
- Disclose the relevant information to the Data Subject (1 month).
- Keep a record of decisions made and information sent (key decisions, exemptions, why conclusions made).

Identify the request and the Data Controller

A Data Subject Access Request (DSAR) can be made in many ways – it does not have to be in writing. The following media could contain a request: telephone call, email, fax, letter, company pages on Social Media. It may be sent to anyone in the organisation, not necessarily the DPO. There is no requirement to mention the Data Protection Act, or DSAR. When we receive a potential DSAR we must also identify who is the Data Controller, in many cases Wealth Wizards may be acting as a Data Processor either on behalf of an Employer utilising MyEva through Wealth Wizards Benefits or a Platform Customer. Where we identify that we are acting as a Data Processor, then we must direct the Data Subject to the Data Controller and notify the Data Controller that a request has been made, however, no further action should be taken without the explicit instructions of the Data Controller. Should we act without the instructions of the Data Controller, we run the risk of becoming a Data Controller by default and this should be avoided at all costs.

Where we are acting as a Data Processor the request may come from a number of channels, this could be a Tess raised by the Platform Customer or as an email from the Data Controller though our Customer Engagement or Client Services Teams. However the request is received we should log and report this request through the process outlined below.

Article 12(6) of the GDPR allows additional information to be requested where the Controller has reasonable doubts as to the identity of the requestor.

If the identity of the requestor is in doubt, obtain ID.

If the DSAR is made on behalf of someone else (i.e. by a solicitor), a letter of authority is needed.

In addition, Recital 63 states:

"Where the Controller processes a large quantity of information regarding the Data Subject, the Controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates."

Log and report internally

When a request is received, advise the DPO who will log internally and diarise the date by which the request must be completed. All DSAR's must be completed within 1 month. The clock starts running when all requested clarification is received and full ID verification satisfactorily completed. Where we are acting as a Data Processor we will liaise and maintain close contact with the Data Controller in order for them to facilitate their obligations to the Data Subject.

The timescale for responding may be extended for a further 2 months, when necessary, taking into account complexity and number of requests. In this case, the Data Subject must be informed of any such extension within one month of receipt of the request, together with the reasons for the delay. (See recitals for specifying which information for large quantities).

The request should be logged in the Platform Service Desk (Tess) as a Data Subject Access Request.

Other considerations

Data

Data held at the time the request was received must not be changed / deleted unless it would have been anyway. In most cases where we are acting as the Data Processor in relation to the Wealth Wizards Platform, the data requested should be supplied to the Data Controller in order for them to add this to any data that they may be supplying to the Data Subject, unless specifically requested by the Data Controller. In some cases where we are acting as a Data Processor in relation to Wealth Wizards Benefits Employers, the data was supplied to us in confidence by the Data Subject, in those instances the information requested should supplied directly to the Data Subject.

Repeat requests

Article 12(5) also provides that the Controller may refuse to act on requests from a Data Subject if they are manifestly unfounded or excessive, in particular because of their repetitive character (or may charge a reasonable fee). The Data Controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

Recital 63 also indicates that an individual should have a right of access *"at reasonable intervals"*, which indicates that, if a reasonable interval has passed, another request may not be considered excessive.

Exclusions

Third party data included with Data Subject information may be excluded, if the identity of the third party could be disclosed. In some cases, redacting the third-party detail may not be enough to prevent the Data Subject identifying the other person. For example, it might be easy to identify who wrote an appraisal form from its style and content. Data Controllers must not only take account of the information they are disclosing, but also of the information which they reasonably believe the person making the request may have, or get hold of, that may identify the third-party individual. In these circumstances, there are two further options which a data Controller could explore:

1. Obtain the other person's consent to the disclosure of their personal date (s.7(4)(a)DPA)
2. Consider whether it is possible to comply with the request without the consent of the third party individual (s,7(4)(b)DPA)

GDPR

Article 15(4) of the GDPR states: *"The right to obtain a copy… shall not adversely affect the rights and freedoms of others."*

Recital 63 refers to the rights and freedoms of others as including trade secrets or intellectual property, but does not refer to information relating to a third-party Data Subject.

Recital 68 states that: *"Where, in a certain set of personal data, more than one Data Subject is concerned, the right to receive the data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation."*

It is not currently clear, therefore, how to deal with third party information under the GDPR, but it appears that a balancing test may still be required between the rights of the requestor and the rights of a third-party Data Subject.

The provision of information in intelligible form

Under Article 12(1) of the GDPR, the information must be provided:

- In a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child
- In writing, or by other means, including, where appropriate, by electronic means. When requested by the Data Subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Under Article 12(3) (relating to all information provided by a Data Controller) and Article 15(3) (relating to providing a copy of personal data being processed), where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided "*by electronic means where possible*" (Article 12(3)) and in a "*commonly used electronic form*" (Article 15(3)).

In addition, Recital 63 states that "*where possible, the Controller should be able to provide remote access to a secure system which would provide the Data Subject with direct access to his or her personal data*".

turo®

BROUGHT TO YOU BY WealthWizards