hasslefree HR

Human Resources & Health and Safety

hasslefree HR

Do you employ staff?

Responding to a Subject Access Request (SAR)

The Right to Access

Individuals have the right to access their personal data, under both the GDPR and the Data Protection Act 2018. This right actually predates the GDPR, as people had the right to access their data under the Data Protection Act 1998, although they had to pay for the privilege. The GDPR updated this right to reflect the fact that no matter who processes the data, a person's data is ultimately their own, and therefore they should not be charged for accessing their own data.

Not to be confused with a freedom of information request, the right to access only applies to an individual's personal data, not wider information about the Company as a whole or information about other employees. Personal data can be defined as any data or information that can directly or indirectly identify a person, both via singular usage (the information on its own) or by being combined with other information. Examples of this would be a person's name, their email address, their payroll identification number, their initials, their National Insurance number, etc. It should be noted that the Information Commissioner's Office warns against a pessimistic attitude when judging if data can identify a person. They advise that if you can distinguish an individual from others, this means they are identifiable.

How to Recognise a Request

There is no specific rule a person must comply with when submitting a request, it could be submitted in writing, verbally, or even over social media! There is also no rule that specifies a person's request must include the wording "subject access request", the only rule is that it must be clear the person is asking for their personal data. So, it is important that you know how to recognise a request when it is received. You can decide to implement your own rules of how a subject access request should be made, such as creating a form for employees to use. However, even if you do create a form an employee can submit a request without using one and should not be penalised or

have the response delayed because of this. The best approach to take would be to assume something is a request and seek clarification if in doubt, rather than ignore or dismiss a comment made by an employee.

Can a Request be Refused?

The majority of subject access requests will need to be complied with, but there are some occasions when a request can either be rejected or delayed for a maximum of three months. If you perceive a subject access request to be “manifestly unfounded” or “excessive”, then you can either completely deny the request or inform the individual that you will provide their personal data within three months rather than one month. A request should only ever be rejected or have an extension applied to it when there is a genuine need or when there are exceptional circumstances, as these decisions do need to be clearly justified. The individual who made the request will need to be clearly informed of the rejection or extension as soon as possible, and they will also need to be informed of how they should lodge a complaint if they disagree with your decision. Current data protection legislation does not clarify what “manifestly unfounded” or “excessive” mean in practice, leading employers to make their own judgement calls, which is another reason to exercise caution here. If in doubt, we would recommend talking through your decision with the ICO, who we know can be very helpful in these situations.

Applying a Fee

Under the Data Protection Act 1998 individuals who wished to access their data were required to pay a £10 charge, regardless of how complex or simple their subject access request may be. However, under the GDPR / Data Protection Act 2018, a person does not have to pay for the right to access their own personal data. The exception is that a small administrative charge can be administered in the event of unnecessary or repeated requests. For example, if one person repeatedly requests the same data, you would be able to apply a charge. This charge should only be for the cost of the administration it takes to respond to the Subject Access Request, so it would only ever be a small amount. The reasoning behind any charge should be clearly explained to the individual who made the request.

Avoiding Accidental Breaches

A common mistake made, when responding to a Subject Access Request, is to provide the individual with everything that includes their data without checking to see if it also includes the data of any other individuals. For example, a customer may provide you with their name and contact details when submitting a review about the level of customer service they received. Part of the review may identify an employee by name, causing the review to become a piece of the employee’s personal data that would need to be provided in response to a Subject Access Request. However, when providing the review it is unlikely that the customer would have agreed to have their name and contact details shared with that specific employee, and therefore if their review was included as part of a response to a Subject Access Request, and the customer’s personal details were not redacted, this may be considered a possible breach of the Data Protection Act 2018. It can be complex and therefore essential that any data processor who responds to a Subject Access Request ensures that any third-party data / personal data they do not have permission to share, is redacted and / or anonymised. It should be noted that personal data is only considered anonymised if there is truly no way to identify the person it refers to; code names etc. rarely count as anonymisation.

Gathering the Data

When an individual submits a Subject Access Request, they are supposed to specify the personal data they are requesting, which makes identifying and providing their personal data relatively easy. However, there will be occasions when a person requests all of their data, and you need to be due diligent with your responses. Personal data should be searched for in the following places:

- Manual filing systems
- Automated filing systems
- Email folders (and other internal communication systems)
- Company websites
- Company newsletters / memo boards
- Payroll department
- Automated security systems (i.e. CCTV systems, facial recognition systems)
- Deleted and archived electronic files

The above list is not exhaustive.

Supplying Data

It is recommended that an individual's data is provided electronically, unless they have requested otherwise. The "best practice" way would be to provide remote access to a secure self-service system, but this is not always possible for all organisations or sectors. Providing the personal data on an encrypted and password protected USB device would be sufficient, although this should be sent separately to the relevant passwords for security purposes. We would also recommend sending an accompanying document that itemises all of the personal data provided, which will make it easier to understand for the individual. Within this accompanying letter, you should also inform the individual of their right to complain if they believe their request has not been properly responded to.

How We Can Help

If you have any queries relating to the content of this newsletter, or any other HR related topic, please don't hesitate to contact us via hradvice@hasslefreehr.co.uk