Professional Indemnity Insurance

New ICO guidance for dealing with Data Subject Access Requests

On 25 May 2018 the General Data Protection Regulations (GDPR)[1] came into force. GDPR was intended to ensure that individuals knew and understood what data was held about them and how it was being used. The impact of GDPR has included privacy notices being updated on websites, the Information Commissioners Office (ICO) issuing significant fines to British Airways and Marriot International and an increase in subject access requests (SARs) across businesses, particularly in London.

SARs are not a new issue under GDPR, they have been in existence since the enforcement of the Data Protection Act 1998. However, the enforcement of GDPR has heightened public awareness about data protection as have the high-profile fines issued by the ICO. What has changed are timeframes for providing information, and the repercussions of not complying.

GDPR reduced the timeframes for responding to a SAR from 40 days to one month. However, in August 2019[2] the ICO announced that the timescale to respond to a SAR has been tightened even further.

The date of receipt is now 'day one' rather than the day after receipt, regardless of whether it is a working day or not. Therefore, a request received on 30 August 2019 must be responded to by 30 September 2019.

This change, whilst minimal, is a useful opportunity to review what to do when a SAR is received, especially as research by Parseq shows that 87% of firms who have witnessed an increase in requests have faced challenges in responding within the timescales. Cost and complexity are cited as the biggest obstacles to responding to these requests.[3]

What is a SAR?

Both the Data Protection Act 1998 and the GDPR recognised that individuals had a right to access their personal data and understand what data was held on them, in order to retain some control over that personal data and how it was used and to whom it might be passed on to. A SAR is a request from an individual to understand what personal data is being held, that it is accurate and how it is being used.

1. GDPR retrieved from https://gdpr-info.eu/
2. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/timescales-for-responding-to-a-subject-access-request/
3. https://www.parseq.com/uk-businesses-are-struggling-to-cope-with-spike-in-gdpr-data-access-requests/

How to recognise a SAR

There is no prescribed method by which a SAR can be made. It could be submitted verbally, in writing or even be made on social media channels. It does not even have to include the phrase 'subject access request'.

It is therefore essential that all staff understand what a SAR is, and what to do if they believe they have received one.

Remember, you only have one month from the day of receipt to respond, so escalation to the correct person is essential at the earliest possible time.

It may be appropriate to have a standard form available for an individual to make a SAR. However, you cannot insist on a form being completed.

"87% of firms who have witnessed an increase in requests have faced challenges in responding within the timescales."

What do I have to do now?

In short you must identify and then provide the personal data to the person who has requested access to it.

It is considered good practice to clarify, in writing, with the data subject (requestor) that you have understood their request, as this will assist in confirming the request is in fact a SAR.

It is further recommended that you keep a record of all SARs received, including when they were received, how they were received, when the Data Protection Officer was notified and the response deadline.

You must further ensure that the information provided is in a concise, transparent, intelligible and easily accessible form. It should be capable of being understood by the average person, and so commonly used acronyms or industry understood jargon (especially in internal documents) may need to be explained.

What are the key differences under GDPR?

You cannot ignore a SAR, if you do you may face the risk of being fined by the ICO.

You can no longer insist on a SAR being made in writing.

Typically, you can no longer charge a fee. Although you may be able to charge an administrative fee if the request is manifestly unfounded, excessive or further copies are requested following an initial request. The ICO provides detailed information on these points.[4]

If the request is made electronically then you should provide the information in a commonly used electronic format.

Other points to consider

Additional Information

You can request additional information to verify identity, but this does not extend the timeframe for providing the information.

Third Party Data

Often legal files will contain personal data about other people. You will need to balance the request against the other individual's rights. This would include considering the type of information being disclosed, whether the other individual has consented to providing the personal data and any duty of confidentiality that you owe.

You may need to consult with a third party and gain their views on releasing this data. Obviously this puts further pressure on the timeframes involved.

Complaint Files

It is possible that you may receive a SAR from a complainant, or where there is possible litigation. Clearly you cannot ignore a SAR on this basis. Equally though you only have to supply personal data under a SAR. Personal data is data that identifies and relates to the individual. The documents in their entirety do not have to be provided; it is only the personal data within the documents that must be provided. Simply because a complaint file exists does not mean that it belongs in its entirety to the complainant. Inevitably there will be personal data within that file that relates to more than one individual. This may then involve reviewing all documentation within a file to decide if it must be provided.

If you do decide to withhold any information due to it being third party personal data, then it would be prudent to keep a record of the decision making and reasoning for doing so.

Again the ICO has provided detailed assistance on this issue.[5]

4. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

5. https://ico.org.uk/media/1179/access_to_information_held_in_complaint_files.pdf

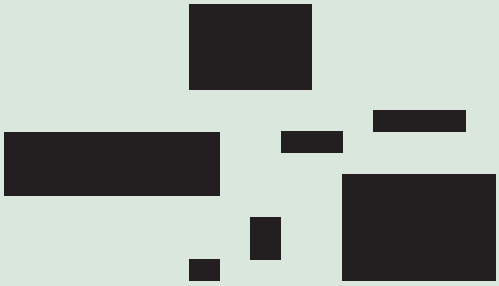
Key Points

- Ensure staff appreciate the importance of and know how to recognise a SAR.
- Know where your data is held, this may include legacy systems or data held with third party suppliers. A data mapping exercise will assist if not already completed.
- Contracts with third party suppliers should include service level agreements that will assist you in responding to a SAR.
- Consider setting up a process and procedure for responding to a request.
- Review how you have responded to a SAR in the past. Consider what worked and what did not. Make any changes to your process to remedy any deficiencies and highlight any good practices, document those changes and the reasons why.

For further information please contact:

John Hosie: Lead Associate, Global FINEX
D: +44 203 124 6742
M: +44 7776 580 169
E: John.Hosie@WillisTowersWatson.com

Willis Towers Watson
51 Lime Street, London, EC3M 7DQ



About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

FPS747 WTW-FINEX 417003/09/19

willistowerswatson.com

Willis Towers Watson