News stories and articles
- General News
- Aviation and Travel
- Clinical Negligence
- Commercial Litigation
- Competition Litigation
- Divorce and Family
- Employment
- International Arbitration
- Investor Protection Litigation
- Personal Injury
- Tax Litigation
- Trust and Probate Litigation

Brochures and publications

A litigator's guide to the galaxy of subject access requests

21 June 2017

Section 7 of the Data Protection Act 1998 (DPA) establishes the right of individuals to make a Subject Access Request (SAR). Individuals can seek access to personal information processed by or on behalf of data controllers and have that - and certain other information relating to the personal data - communicated to them, subject to specific exemptions set out in the DPA.

The DPA transposes into English law the EC Data Protection Directive (94/46/EC), the primary objective of which is to protect individuals' fundamental rights. This includes the right to privacy and the right of access to personal data in order to verify the accuracy of the data and the lawfulness of the processing. A data controller under the DPA broadly encompasses any organisation that processes data or makes decisions about the processing of data. As such, SARs have commonly been used by individuals to gain access to personal information from a wide array of organisations who process data on a regular basis such as employers, businesses, health authorities and the police.

In recent years there has been an increased use of SARs within the context of civil litigation to obtain information which might not otherwise be disclosable or at an earlier stage than would ordinarily be the case, as part of an overall litigation strategy. There has been a simultaneous development of case law as to the correct interpretation of the provisions of the DPA and the legitimate parameters of SARs. The approach taken by the court in a number of cases, has been that when determining whether to exercise its discretion pursuant to s7(9) DPA to order compliance with a SAR, the court would consider an individual's motivation or purpose for making a request to access data. In circumstances where the purpose of the request was to verify the accuracy of personal data or the lawfulness of the processing but also included a collateral purpose to obtain material for use in litigation, the request could be found to be a misuse, or not a proper use of the DPA. Applications seeking the enforced compliance of reluctant data controllers could therefore be dismissed on these grounds. This caused a degree of uncertainty both for data subjects as to the limitation of their right of access and for data controllers as to the grounds on which compliance with a SAR could be resisted.

In a string of recent judgments - Dawson-Damer v Taylor Wessing LLP [2017] and the joined appeals of Deer v University of Oxford and Ittihadieh v 5-11 Cheyne Gardens [2017] - the Court of Appeal has clarified the law in relation to SARs. This goes some way towards reconciling the tension that had arisen between the court's approach and that of the Information Commissioner's Office (ICO)[1] as set out in the ICO's Code of Practice on subject access (the Code of Practice). In the light of this latest development in the field of data protection, this article provides an overview of the merits and limits of SARs as a tool in civil litigation as well as the practicalities to consider when making or receiving them.

The merits of SARs in civil litigation

Ease of use and cost

Making a valid SAR is straightforward and inexpensive. There is no prescribed format provided it is in writing - indeed the Code of Practice specifies that data controllers may not insist on the use of a particular form. A written SAR can be made by post, email, fax and even on social media. It does not have to be labelled as a SAR, nor make any reference to the DPA. Generally, the maximum fee that can be charged by data controllers for dealing with a SAR is £10. A response must be provided promptly and in any event within 40 calendar days from the date of receiving the request. Where the request is made by a third party on behalf of the data subject, for instance through a solicitor (as is often the case), the data controller must be satisfied as to the identity of the requester and may ask for information confirming this - such as a letter of authority on behalf of the data subject or a power of attorney. For data subjects, it is important not to fall foul of these requirements when making the request as the 40 day long-stop date does not commence until these have been satisfied. Data controllers need to be mindful of the importance of verifying the identity of the requester where appropriate to ensure it is a genuine request made by the correct data subject. It should be noted that the General Data Protection Regulation (GDPR) which is due to come into force on 25 May 2018 will make some changes to the law relating to SARs. One of the main aims of the new data protection framework is to bolster the rights of individuals as evidenced by measures such as

contactus

Faranak Ghajavand
Solicitor in the Commercial Litigation Department, Stewarts Law LLP
T: +44 (0)20 7822 8174

Email Faranak

News

David Hughes joins Stewarts Law as partner in the Commercial Litigation team
05 June 2017
David brings with him a wealth of experience, in particular advising governments, sovereign funds and institutiona.....

Tesco shareholder action forges ahead – CDR Magazine article
25 April 2017
CDR Magazine provide an update on the legal action against Tesco by their shareholders...

Contractual interpretation: Through the looking glass... once again?
20 April 2017
Paul Brehony and William Gow of Stewarts Law consider the pendulum of case law in contractual interpretation....

Disclosing the identity of third party funders
04 April 2017
Two recent cases confirm the court's jurisdiction to order the disclosure of the identity of commercial third part.....

Group Litigation Orders: Lessons from the RBS Rights Issue Litigation
13 March 2017
In theory group litigation orders corral claimants into one easy-to-manage group. In practice this is often somewh.....

See also

Commercial Litigation

reducing the time within which data controllers must respond to one month, removing the right to charge a fee and substantially increasing the potential penalties data controllers could face for non-compliance.

The information that individuals are entitled to request from data controllers pursuant to the DPA is:

- Whether (and if so) what personal data are being processed by or on behalf of the data controller.
- A description of (i) the personal data, (ii) the purposes for which they are being or will be processed, and (iii) the recipients or classes of recipients to whom the data may be disclosed.
- Copies of the personal data in an intelligible form and information on the source of the data.
- The extent to which the data controller is using the data to make automated decisions relating to the data subject (such as performance, creditworthiness or conduct) and, if so, the logic behind such decisions.

The process has been designed to be straightforward and can be followed by reference to the DPA and the Code of Practice. One potential source of complication is that the request must include information that the data controller may reasonably require to enable it to locate the personal data being sought; the data controller need not comply with the SAR until this has been provided. As the Code of Practice makes clear, this is not a get-out clause on the part of organisations to delay or avoid responding to requests until the scope has been narrowed down. Where possible, data controllers should respond to those parts of the SAR that are clear and, if there are good reasons to do so, ask for more information from the data subject in order to provide a full response. In practice, whether or not a data controller has the information it reasonably requires in order to respond will depend on the circumstances. If a limited amount of data is held relating to an individual, a simple request asking for access to all data held by an organisation relating to that individual may be reasonable. In other circumstances, it can be reasonable for an organisation to ask for information as to the type of electronic data being sought and an estimate of the dates it was created.

Methods of enforcement

One of the key aspects of the subject access regime and the merits of its use to litigants or potential litigants is the availability of routes to enforcement when data controllers do not comply or adequately engage with a SAR that has been made. Data subjects can turn to the ICO and/or the courts and the main remedies available are:

- A request to the ICO to assess whether it is likely or unlikely that the processing of data is being done in compliance with the DPA. This is called a compliance assessment. Where the ICO's assessment is that an organisation has failed or is failing to comply with the DPA, it can ask the organisation to take steps to remedy this, including where appropriate, an order for it to do so.
- The service of an enforcement notice by the ICO on a non-compliant data controller. Failure to comply with such an enforcement notice is a criminal offence. The Code of Practice states that before serving an enforcement notice, the ICO has to consider whether the non-compliance has caused or is likely to cause damage or distress. Where this is not the case, it must nonetheless be reasonable to serve an enforcement notice but the Code makes clear the ICO will not ask organisations to take unreasonable or disproportionate steps to comply with SARs. It is important to bear in mind that the ICO has no power to award compensation to individuals; it has a statutory power to impose a financial penalty on organisations of up to £500,000 where a serious breach of the DPA has been committed.
- An application to the court pursuant to s7(9) DPA alleging breach of the subject access rules and seeking an order for compliance. The court has discretion whether to make such an order. The well-established position in the authorities - going back to the landmark data protection case of Durant v FSA [2003] - is that the court's power under s7(9) is generalised and untrammelled. Whilst awards for compensation under the DPA have historically, in general, been low, the benefit to those using the subject access regime is the existence of a long line of authority to guide data subjects and their advisers when faced with the prospect of an application to court to seek enforcement. These demonstrate how the court has interpreted the subject access provisions and, specifically, the circumstances where it has exercised its power to order compliance.

No 'no other purpose' rule

Until the Court of Appeal's recent judgment in Dawson-Damer, the authorities seemed to support the position that, when deciding whether

to exercise its discretion pursuant to s7(9) DPA, the court could look at the purpose and motivation behind the making of a SAR. Dawson-Damer concerned a SAR that had been made by beneficiaries under various Bahamian trusts to a firm of solicitors who represented the trustee, requesting access to all data of which the beneficiaries were the data subjects. The solicitors did not provide copies of the personal data relying on exemptions under the DPA. The beneficiaries applied to the court for an order of compliance under s7(9) DPA. A few months later, the beneficiaries commenced proceedings against the trustee in the Supreme Court of the Bahamas. This gave rise to an issue as to whether the purpose behind the SAR was to verify the accuracy of the beneficiaries' personal data held by the trustee and to seek access to information that could not be obtained through disclosure in the ordinary course of the Bahamian proceedings. Dismissing the beneficiaries' application for enforcement, one of the reasons provided by the first instance judge (His Honour Judge Behrens) was that it is not the purpose of s7 DPA to enable an individual to obtain disclosure of documents that may assist him in litigation or complaints against third parties. The judge relied on Auld LJ's judgment in Durant at paragraph 27. Dealing with how the s7(9) discretion should be applied, the judge held that no order should be made if the data subject intended to use the information obtained to verify or correct data (that is, a proper purpose behind the data protection principles), but also wanted the data to assist him in other proceedings (which would be a misuse of s7).

This has been referred to as the 'no other purpose rule': that there is an implied rule in the DPA (established in Durant and applied in Dawson-Damer [2015], (see also Kololo v Metropolitan Police Commissioner [2015])) that a data subject should not exercise DPA rights for purposes outside the DPA. Some observers had raised a concern that this approach had a potential to constrain the rights to subject access under section 7 by reference to proper and improper purposes which went beyond the exemptions to those rights set out in the DPA itself. The Court of Appeal in Dawson-Damer has now clarified the matter, determining that Durant is not authority for a 'no other purpose rule', and ruling that a SAR would not be invalid if it had been made with the collateral purpose of assisting with litigation. Delivering the leading judgment, Arden LJ noted (at paragraph 107) that the EC Data Protection Directive "makes it clear that the rights given by the Directive are to protect fundamental rights conferred by EU law. We have been shown nothing in the DPA or the Directive which limits the purpose for which a data subject may request his data, or provides data controllers with the option of not providing data based solely on the requester's purpose".

Prior to the Court of Appeal's decision, the approach taken by the court seemed to be inconsistent with that of the ICO, as stated in the Code of Practice:

> It has been suggested that case law provides authority for organisations to refuse to comply with a SAR where the requester is contemplating or has already begun legal proceedings. The Information Commissioner does not accept this view, but he recognises that (i) the courts have discretion as to whether or not to order compliance with a SAR; and (ii) if a court believes that the disclosure of information in connection with legal proceedings should, more appropriately, be determined by the Civil Procedure Rules, it may refuse to order personal data to be disclosed. Nevertheless, simply because a court may choose not to order the disclosure of an individual's personal data does not mean that, in the absence of a relevant exemption, the DPA does not require you to disclose it. It simply means that the individual may not be able to enlist the court's support to enforce his or her right.

As such, data subjects faced with reluctant data controllers had reason to hesitate before applying to the court for an order for compliance if they were litigants or potential litigants and the exercise of their right to subject access could be seen as an attempt to misuse s7 DPA. With the Court of Appeal's ruling that there is no 'no other purpose rule' implied in the DPA which would act as an automatic bar to the court's exercise of its s7(9) discretion, it would seem that data subjects who are - or may become - engaged in legal proceedings can exercise their DPA rights with a greater degree of certainty.

Faranak Ghajavand is a Solicitor in the Commercial Litigation team. She specialises in complex and large-scale commercial dispute resolution. She has a broad range of experience acting for both claimants and defendants in domestic and international disputes, whether by way of litigation, commercial or investment treaty arbitration.

Faranak's cases include defending a US client in a $1bn indemnity claim in the Commercial Court regarding the contamination of a river in the US and assisting on a claim brought by a group of leading UK retailers against Visa and MasterCard regarding interchange fees. She has also advised on a matter involving serious allegations of fraudulent misrepresentation and conspiracy surrounding a repurchasing agreement, successfully obtaining a $20m High Court Court judgment and a worldwide freezing order.

Back to top | Print page