Data Subject Access Requests — three illuminating UK cases

Kate Brimsted, Partner and UK Head of Data Privacy and Cyber Security, and Tom Evans, Associate, with Bryan Cave Leighton Paisner, highlight three cases in the UK which illustrate the current trends and issues with DSARs

Like the proverbial bus, data protection specialists can wait a while for a significant case on data subject access requests ('DSARs') only to find that several come along in close succession! This article highlights three English court judgments and an Upper Tribunal decision, all of which apply the pre-GDPR legal framework though they illustrate trends and issues which are equally relevant under the current law.

Individuals seeking to enforce their access rights in the English courts have met with varying degrees of success over the years. In early cases such as *Durant v Financial Services Authority 2003*, senior judges derided the 'misguided' attempts of claimants to "use the machinery of the [Data Protection Act 1998] as a proxy for third party discovery with a view to litigation". However, for almost a decade now the right of access to personal data has been a fundamental human right in EU law, as enshrined in Article 8 of the EU Charter of Fundamental Rights. More recent cases, together with a maturing of the data protection legislative environment and a change in societal attitudes towards 'data' and individual autonomy, have indicated a marked shift towards those making DSARs.

The cases described below demonstrate the significant lengths to which controllers are now expected to go when responding to a valid DSAR. It is notable that each of these decisions were made under the Data Protection Act 1998 (the 'DPA 1998') which was the law in place before the General Data Protection Regulation ('GDPR'). Given the boost to individuals' rights provided by the GDPR, along with the increased accountability and transparency obligations for controllers, the direction of travel suggests this most powerful right will pose increasing challenges for compliance.

A session on 'The Changing Face of Subject Access under the GDPR' features on day 1 of the 18th Annual Data Protection Practical Compliance Conference, taking place in London on 10th and 11th October. See the website for details www.pdpconferences.com

Dawson-Damer: 'Relevant filing system', reasonable and proportionate searching and consistency when withholding information

On 19th May 2019, judgment was given in the latest instalment in the Dawson-Damer trusts litigation (*Dawson-Damer v Taylor Wessing* [2019] EWHC 1258 (Ch)) which saw the High Court consider some fundamental concepts for DSARs.

The underlying dispute arose from the restructuring of a number of private family trusts in a manner which the claimants felt unfairly disadvantaged by. In 2014, DSARs were made by the claimants, who are beneficiaries of the trusts. The English solicitors advising the trustees, TW, also received DSARs from the beneficiaries. Trust-related litigation was then brought in the Bahamas against the trustees.

In responding to the DSARs, TW asserted that all personal data of the claimants held by them was covered by legal professional privilege ('LPP') and therefore exempt from disclosure. The claimants applied to the English High Court to request that the court exercise its discretion to order TW to comply with the DSARs. At first instance, the judge considered that the LPP exemption applied, and that any further search by TW would be disproportionate. The court ruled that it would not exercise its discretion to order a response to the DSARs, because the real motive was to use information in the Bahamas in proceedings, and this was not a proper use of the DSAR process. The matter was appealed in 2017 and overturned by the Court of Appeal on all three points. Following that, it was remitted back to the High Court and judgment given in May 2019.

The main points determined were whether the paper files maintained by TW before it moved to electronic files in 2005 were a 'relevant filing system' and whether TW had breached its obligations by failing or refusing to carry out a reasonable and proportionate search and by redacting or withholding the claimants' non-exempt personal data.

Whether the paper files constituted a 'relevant filing system' under the DPA 1998

This question is fundamental when it comes to determining the kind of material which comes within the scope of a DSAR. This is because, generally speaking, information held solely in paper files (sometimes called 'manual data') is in scope only if it is part of a 'relevant filing system', meaning that the information is organised in such a

way as to allow specific information about particular individuals to be readily accessed. (A similar principle also applies in the GDPR, within the definition of 'filing system'). In this case, the solicitors held paper files dating back many years. One set of 35 files was described as relating to the 'Yuills Trusts' containing correspondence in chronological order and some documents which were not date sorted.

The court held that the information was held in a 'relevant filing system', meaning the solicitors were required to search the files for any personal data of the claimants.

This was a departure from the narrow finding of 'relevant filing system' in *Durant v Financial Services Authority,* with the court favouring the wider test set out by the CJEU in *re Tietosuojavaltuutettu* (Case C-25/17). The Judge noted that the *Durant* case was decided before the right to protection of personal data was enshrined as a fundamental right in EU law and that the perspective on the right to protection of personal data has altered: the focus is now on the need for protection of the data subject as opposed to the burden on the controller. The Judge specifically commented that the level of protection that right has received in the English courts has increased, and it was unduly restrictive and could create a serious risk of circumvention, to apply the *Durant* approach, i.e. requiring that there must be a structured referencing mechanism, containing a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file specific criteria or information about the applicant can be readily located.

As the category of files in question clearly related to trusts in which the claimants, or at least the first claimant, was a potential beneficiary, the court held that description was a criterion which allowed access to their personal data. Giving the words 'relating to individuals' an extensive interpretation, the court found that the fact that the files related to trusts in which one or all of the claimants were potential beneficiaries, was sufficient to satisfy that requirement. The question of whether the specific criteria enabled the data to be 'easily retrieved' was then considered. The Judge noted that the files in question were arranged in chronological order and it would require someone to turn the pages to locate the personal data. Having a trainee turn the pages of the files to identify personal data and then having it reviewed by a senior associate was not unduly onerous, and therefore enabled any personal data of the claimants to be 'easily retrieved'.

The judgment suggests that respondents to DSARs will likely be expected to consider all files, regardless of their physical format, where they are organised in some meaningful fashion that allows both identification of the data subject and the structured searching of the documents. The GDPR includes a definition of 'filing system' at Article 4(6) and it is reasonable to expect that this will be construed accordingly.

What amounted to 'reasonable and proportionate' searches for personal data?

The court found that TW had failed to provide evidence establishing the time and cost involved in conducting a further search for the claimants' personal data, meaning TW did not discharge the burden of showing that such a search would be disproportionate. It also appeared to be to the claimants' advantage that they had produced a targeted list of further searches and the court held that TW had not discharged its burden of showing all of these further searches would be disproportionate.

The judgment affirms that the burden is on the controller to prove that it has discharged this, and that giving an indication of cost or time that would be entailed in going beyond what had been undertaken could be helpful. The court firmly rejected the argument that the claimants' motivation to use the DSARs as an additional disclosure exercise in relation to the Bahamian trust proceedings was a relevant factor in deciding what was 'proportionate' (or not).

The ruling may impact future interpretation of Article 12(5) of the GDPR, which provides that where requests made by a data subject are 'manifestly unfounded or excessive' the controller may either charge a reasonable fee for its services or refuse to act. The controller is obligated to 'bear the burden of demonstrating the manifestly unfounded or excessive character of the request'. This judgment underlines this last point, suggesting courts will take seriously a controller's evidential burden in justifying a refusal to answer a DSAR. In this sense this judgment appears to foreshadow the accountability requirements of the GDPR and Article 12(5).

Redaction and the withholding of personal data

The court examined a small sample of redacted documents which the claimants indicated demonstrated an inconsistent or incorrect approach to redaction; the Judge then ruled that it was clear in some instances there had been more redaction than there should have been. Unfortunately for TW, the court found the appropriate course was for TW to review the other redactions it had made and apply the principles arising from the Judge's examination of the samples, ensuring consistency of approach.

The judgment also discussed the application of the LPP exemption in the context of trust law and the applicability of law (English and Bahamian).

Green v SCL Group: The special role of insolvency practitioners

On 17th April 2019, the High Court confirmed in this case (*Vincent John Green, Mark Newman (as joint Administrators of each of the Companies) v SCL Group Limited, SCL Analytics Limited, SCL Commercial Limited, SCL Social Limited, SCL Elections Limited, Cambridge Analytica* (UK) Limited [2019] EWHC 954 (Ch) that administrators (like liquidators) are not 'controllers' of personal data, meaning they are not required to respond to DSARs issued against the companies over which they have been appointed.

(Continued on page 8)

(Continued from page 7)

In the aftermath of the Cambridge Analytica scandal, numerous companies within the Cambridge Analytica group suffered severe financial losses and administrators were appointed. Unknown by the administrators at the time of their appointment, the situation had been compounded by the seizure by the Information Commissioner's Office (the 'ICO') of the companies' equipment and servers, meaning they were unable to continue trading. A creditor in the US, Professor Carroll ('C') had made DSARs which had not been responded to, and the ICO then issued Enforcement Notices against the company. Following a failed administration process, the administrators requested that they be appointed liquidators of the various companies.

The creditor's DSARs

C objected to the appointment of the administrators as liquidators, asserting that the administrators had breached duties they owed to data subjects under data protection laws, as well as making objections based on insolvency law. The creditor had made a DSAR to two group companies, requesting details of his personal data. After no response was provided, C's complaint to the ICO led to Enforcement Notices being issued under the Data Protection Act 1998 to compel compliance with the DSARs. The companies were subsequently prosecuted for failure to comply with the Enforcement Notices.

The data protection status of administrators

In referring to established case law, the High Court noted that liquidators who operate as agents on behalf of a company cannot be controllers of personal data unless the liquidator takes decisions about the processing of personal data as principal. The court found the same reasoning also applies to administrators.

In a ruling which will be of great relief to liquidators and administrators concerned about the possible broadening of their own administrative duties, the court also held that neither liquidators nor administrators are obligated to investigate breaches of data protection law by a company. The court determined that any data protection investigations should remain within the purview of external regulators, such as the ICO in the UK.

Rudd v Bridle: application of exemptions and extent of transparency information

On 10th April 2019, the High Court ruled in *Rudd v Bridle* [2019] EHC 893 (QB) that information provided to the claimant, Dr Rudd, in response to a DSAR made by him under the DPA 1998 had been inadequate. The court ordered significant further disclosure by the recipient of the DSAR.

Dr Rudd is a medical doctor specialising in the science of exposure to asbestos and the causal connections with lung diseases. He has given expert evidence in many cases over the last 35 years in which claimants have sought damages allegedly caused by exposure to asbestos.

The defendant, Mr Bridle, formerly worked in the building industry, including manufacturing products containing asbestos; he now runs a company, Asbestos Watch, which appears to undertake lobbying on behalf of the industry. Dr Rudd and Mr Bridle profoundly disagree regarding the role of asbestos in causing disease, and Mr Bridle called into question Dr Rudd's conduct in his role as expert witness in cases claiming damages for disease attributed to asbestos exposure. Mr Bridle made complaints to the GMC, the Justice Secretary and Members of Parliament, alleging that Dr Rudd was part of a conspiracy with claimant law firms. Dr Rudd made DSARs in this context to Mr Bridle and also to Asbestos Watch. In addition to the core right to access in response to a DSAR, there was (and still is under the GDPR/DPA 2018) the right for the maker of the DSAR to receive information connected with the processing of his personal data, e.g. the source of the information and the purposes of the processing. (This requirement has been significantly extended in Articles 12 and 15 of the GDPR).

The Judge described the parties' approach in the case as not only fractious, but undisciplined and disorderly, bordering at times on the chaotic. The main issues raised were summarised as (1) the controller issues; (2) the subject access issues — the exemption issues and the adequacy issues; (3) the unwarranted processing issues; and (4) the remedies issue. A number of these are described below. The court exercised its discretion to order Mr Bridle to provide further information to Dr Rudd.

The identification of third parties

The court decided that the identities of the third parties with whom Dr Rudd was alleged by Mr Bridle to have conspired was the personal data of Dr Rudd, as the data was focused on Dr Rudd and was biographically significant. This information therefore had to be disclosed.

In contrast, the court held that there was no obligation to disclose the recipients who received emails from Mr Bridle containing the personal data of Dr Rudd. The court held that the DPA 1998 and the ICO's Subject Access Code state that a DSAR applicant should be provided with a description of the recipient and not their identity/name.

The application of exemptions to providing information

The court held that the fact Mr Bridle's solicitor had reviewed the relevant materials, and determined that an exemption to disclosure applied, was not conclusive. A court will often not exercise its discretion to order disclosure where the controller has acted with reasonable diligence in determining that an exemption applies and there is no substantive reason to doubt their conclusion. In this case, however, the court held that none of the exemptions which Mr Bridle sought to rely upon applied, namely: journalism, regulatory activity or litigation privilege (though a claim for legal advice privilege was accepted). The court held that the regulatory exemption can apply where personal data are processed for the purpose of regulatory functions and such processing is carried out by a regulatory body itself, as opposed to where personal data is processed by an individual who plans to report to a regulator.

(Substantially the same exemptions also appear within the DPA 2018 at Schedule 2).

The regulatory exemption was also determined to apply only to the extent that providing personal data pursuant to the DSAR could prejudice the regulator's capacity to properly carry out its regulatory functions. (The DPA 2018 includes language to the same effect at Schedule 2, Part 2, paragraph 11).

The sources of the personal data
The court held that controllers must provide any information they have available to them concerning the source of the individual's personal data. Mr Bridle had taken a blanket approach to the identification of third parties (to resist this). The provisions in section 7 DPA 1998 relating to information which could identify other individuals, cannot be relied on to withhold the identities of any firm, company or other legal entity, e.g. the names of the solicitors' firms involved. As to personal information about sources, the court noted there was no evidence that anybody had been asked for their consent (or refused it).

The purpose of data processing

The court held that the requirement to disclose the purpose of processing need not occur on a document by document basis, as the claimant had contended; the controller which receives the DSAR can set out the general essence of what the controller was doing with the data.

Campbell v Secretary of State: Access requests after death

This case arises out of three test cases brought on behalf of 100 individuals seeking access to official records about their internment without trial in Northern Ireland in the 1970s. The matter was an appeal from the General Regulatory Chamber of the First-tier Tribunal. Following the death of Mr Campbell in 2015, one of the three individuals who had made a DSAR for this purpose, the Upper Tribunal (Administrative Appeals) ('UT') was required to determine: (i) whether Mr Campbell's right of access to his personal data had survived, and (ii) whether his rights to appeal against a national security certificate issued by the Secretary of State under section 28(2) of the DPA 1998 (which exempted the records from access under a DSAR) had survived.

The UT determined that the deceased's right of access was a purely personal and independent right. The right was therefore incapable of withstanding his death and could not give rise to a cause of action for his estate. It was held that rights relating to DSARs are not rights to be exercised by third parties, regardless of their relationship with the deceased.

The UT found that the right of appeal against the issuance of a national security certificate was nothing more than a statutory appeal route. This was therefore not a freestanding right of appeal, and did not amount to a cause of action. As it was not independent of the DSAR right, it did not survive Mr Campbell's death.

Decisions of the UT are not binding on the High Court although have precedential value equivalent to a High Court judgment. This case is certain to influence the interpretation by the UK courts of both an individual's DSAR rights under Article 15 of the GDPR and the national security and defence exemptions contained in sections 26 and 27 of the DPA 2018 (and the associated statutory appeal mechanism). The appeal right against the issuance of a national certificate contained in section 28(4) of the DPA 1998 has also been replicated at section 27(3) of the DPA 2018, underlining that the approach adopted in this case can be expected going forward.

Some practical points

Relevant filing systems may be of limited practical application given the prevalence of digitised information and records; however, the widened concept could be of concern for organisations which retain significant paper records. Relying on an argument that the paper records do not have to be considered for the purposes of a DSAR on the grounds that they do not amount to a 'filing system' for GDPR purposes appears considerably less secure than previously thought.

Courts can be expected to be more 'hands on' when it comes to examining the approach taken by a controller to redactions where the maker of a DSAR challenges the consistency (or extent) of information withheld. This review is likely to be confined to a 'sampling' exercise, but the parameters of that sample may be dictated by the maker of the DSAR, as the party complaining about the execution of the process.

A controller may therefore find itself re-running the DSAR, which could be a significantly time-consuming and costly exercise.

It is for a controller contending that the search has been 'reasonable and proportionate' to prove this; in practice that may mean providing evidence as to the (disproportionate) effort which further searching would require. The dissatisfied maker of a DSAR may attempt to put the controller on the 'back foot' by submitting a list of further searches which could/should be undertaken, which the controller then has to prove would be disproportionate to conduct.

The ICO's updated Subject Access Code for the post-GDPR environment is currently awaited. Traditionally, the ICO's position on DSARs has tended to be considerably more demanding than the courts. Now that the court's stance has hardened, controllers may be forgiven for anticipating the ICO's update to the Code with a degree of trepidation.

We would like to thank Jack Dunn, trainee solicitor, for his assistance with this article.

Kate Brimsted and Tom Evans
Bryan Cave Leighton Paisner
kate.brimsted@bclplaw.com
tom.evans@bclplaw.com