Subject access: the battle lines are redrawn

DANIEL POLLARD, GQ Employment Law LLP and CHRISTOPHER STONE, Devereux Chambers

Subject access requests have become a standard weapon in the claimant's armoury. Since the Court of Appeal's decision in Durant there has been uncertainty about whether a data controller will be compelled to comply if the SAR is used for obtaining pre-action disclosure and as to the scope of the 'disproportionate effort' exception. Clarity has now been given by two separate constitutions of the Court of Appeal in Dawson-Damer and the conjoined cases of Ittihadieh/Deer. The Information Commissioner intervened in both cases.

The subject access right

An individual has a right to make a request for his or her personal data under s.7 DPA. In response, a data controller is obliged by s.7(1)(c) to 'communicate to him in an intelligible form the information constituting any personal data of which that individual is the data subject'. There are numerous exemptions and exclusions from this right, which, save for the exception for privileged materials under Schedule 7, fall outside the scope of this article.

If a data subject considers that the data controller has failed to comply with this duty, he or she can bring a claim under s.7(9) DPA asking the court to require the data controller to comply with the request. He or she can also potentially claim compensation for any damage or distress suffered by the failure to comply under s.13 DPA. He or she can also complain to the Information Commissioner's Office (ICO), which has extensive enforcement powers which it exercises in line with its regulatory action policy.

An important qualification on a data controller's obligations is contained in s.8(2)(a) DPA – a data controller does not have to supply data in permanent form if 'the supply of such a copy is not possible or would involve disproportionate effort'.

The DPA implements Directive 95/46/EC. The right of data access is contained in article 12. The purpose of that right is explained in recital 41: 'In order to verify in particular the accuracy of the data and the lawfulness of the processing.' The concept of a 'collateral purpose' has therefore been used in the authorities to mean a purpose that is unrelated to checking the accuracy of the data held by the data controller or ensuring that it complies with the data protection principles; for example, making a SAR for the purpose of obtaining pre-action disclosure related to other proceedings.

What is personal data?

A data controller's duties under the DPA are engaged only if it processes 'personal data', and so this must be considered as a starting point when responding to a SAR.

Ittihadieh/Deer followed *Durant* and the judgment of the CJEU in *YS* in applying a restrictive interpretation of personal data and in stressing the distinction between seeking documents and accessing personal data – those who seek documents are 'aiming at the wrong target'. Following *Ittihadieh/Deer,* data controllers should consider whether it is more appropriate to respond to a SAR by providing a schedule of personal data rather than copy documents (suitably redacted where necessary).

Does a collateral purpose invalidate a SAR?

In *Durant*, which until now was the leading authority on many aspects of handling SARs, Auld LJ said that a SAR is not to

'the purpose of a SAR can be taken into account by a court as a relevant factor when exercising its discretion under s.7(9)'

assist a data subject 'to obtain discovery of documents that may assist him in litigation or complaints against third parties'. That quote has often been cited as authority for the proposition that a data controller is not obliged to comply with a request if it is made for a collateral purpose. The ICO has always disagreed: the SAR code says that 'there is nothing in the Act that limits the purposes for which a SAR may be made, or which requires the requester to tell you what they want the information for.'

S.7(9) of the DPA gives the court the discretion whether to order compliance with a SAR. In the High Court in *Dawson-Damer*, HHJ Behrens QC said that if required to do so he would have used his discretion against requiring compliance with the SAR because the data subject's purpose of obtaining disclosure in other proceedings was 'not a proper purpose'.

The Court of Appeal in *Dawson-Damer* found that that approach was wrong. Arden LJ relied upon the fact that there is nothing in the DPA or the Directive that requires a purpose to be stated or which limits the purpose for which a request for data can be made. *Dawson-Damer* therefore clarified that a collateral purpose in making a SAR is not an ***automatic*** bar for refusing to comply. The court in *Ittihadieh/Deer* reached the same conclusion.

Discretion

Although a collateral purpose does not invalidate a SAR, in *Ittihadieh/Deer* Lewison LJ said that the purpose of a SAR can be taken into account by a court as *a* relevant factor when exercising its discretion under s.7(9). A data controller will therefore still be able to argue that even if it failed to comply in full with its duties under the DPA, the data subject should not be entitled to the remedy sought because of the purpose for which he has brought the SAR.

As an aside, a collateral purpose was also held by the Court of Appeal to be a relevant factor in making an award of costs in the data controller's favour, notwithstanding that the court found it had breached its duties under s.7.

The one area of apparent inconsistency between Arden LJ in *Dawson-Damer* and Lewison LJ in *Ittihadieh/Deer* is the correct starting point for the application of the court's discretion. Arden LJ followed *Durant* in holding that the court has a 'general' discretion. She specifically rejected the submission of the ICO that there is a presumption in favour of ordering compliance with the SAR. In contrast, Lewison LJ endorsed an approach that the discretion should be exercised in favour of the data subject absent a good reason not to. Factors that may mitigate against ordering compliance include if:

- other legal proceedings offer a more appropriate route to disclosure;
- the breach is trivial;
- there is not a 'legitimate reason' for the SAR (for example, to check the accuracy of the data held);
- the SAR is an abuse of rights (for example, it is intended to burden the data controller) or procedurally abusive (for example, because it has failed before);
- the real request is for documents and not personal data;
- the information sought would not be of real benefit to the data subject – considered further below;
- the SAR was disproportionate; or
- the data subject has already received the data.

Disproportionate effort

The Court of Appeal has also re-evaluated 'disproportionate effort'. The starting point is the meaning of 'supply' in s.8(2)(a) because the limitation only applies if the 'supply' of a copy of the data would involve disproportionate effort. Arden LJ found that that cannot be limited to just the effort in copying the documents, but instead it must be the entire effort that leads to the final supply of the data.

In *Dawson-Damer*, the data controller had produced no evidence of having carried out any search for the claimant's personal data. Following the Court of Appeal's judgment, if a data controller has some personal data of the data subject, it will very rarely, if ever, be advisible to make no effort to respond.

The Court of Appeal in *Ittihadieh/Deer* agreed with this approach, although it appears that that court would have derived the limit on a data controller's obligations from the general EU principle of proportionality rather than the words of s.8(2)(a) itself. Lewison LJ observed: 'The EU legislature did not intend to impose excessive burdens on data controllers'.

This aspect of the courts' judgments will be welcomed by employers and is significant because it is the process of reviewing automated keyword search results within unstructured electronic data sources to determine whether personal data exists, extracting that data and applying the various exceptions that makes responding to SARs so onerous and expensive. This is a process that (as recognised by Lewison LJ in *Ittahdieh*) must be performed manually – at least for now.

'the ICO has in recent years acknowledged that there is a (limited) element of proportionality in relation to the entire process of responding to a SAR'

The question of disproportionate effort begs the question: 'Proportionate to what?' Arden LJ is clear: the data controller must balance the effort that will be involved in finding and supplying the information sought on the one hand, against the benefit that supply of the information would bring to the data subject on the other.

Arden LJ specifically endorsed *Ezsias* as a correct approach to the necessary proportionality balancing exercise. In *Ezsias,* Judge Hickinbottom found that the Welsh Assembly had carried out a reasonable and proportionate search, taking into account the fact that the data subject would in any event receive all the documents that he sought through his SAR as disclosure in his parallel employment tribunal proceedings. *Ezsias* was also endorsed in *Itthadieh/Deer*.

Some examples to give a sense of the scale of the exercises undertaken in responding to SARs are set out in the box, below.

ICO code of practice

The ICO has in recent years acknowledged that there is a (limited) element of proportionality in relation to the entire process of responding to a SAR and the SAR code acknowledges that employers are not required to do things that would be unreasonable or disproportionate. Practitioners will be well used to citing the conflicting provisions of the SAR code, although its overall tenor perhaps suggests that the duty imposed on data controllers is more onerous than suggested by *Dawson-Damer*. The ICO may disagree with that view, but it is noteworthy that Arden LJ did not take the opportunity to endorse the SAR code. Many employers, particularly those in regulated industries or with consumer-focused databases, will be more concerned by regulatory action by the ICO than they will a claim under s.7(9). It will be interesting to see whether the SAR code is now updated.

Privilege

In *Dawson-Damer,* the data controller was a firm of solicitors that asserted that many of the documents containing the data subject's personal data were covered by legal professional privilege in Bahamain proceedings. The Court of Appeal held that the exeption in schedule 7 only applies to documents which may be privileged in UK proceedings. The interplay between the scope of privilege in the UK and in overseas jurisdictions may be of interest to solicitors with such clients but is outside the scope of this article. The Court of Appeal was clear that a broad assertion that most documents were covered by privilege is not sufficient to avoid the data controller's obligation to conduct a search at all, although it may be relevant when considering the proportionality of that search.

The court in *Itthadieh/Deer* has said that there is no obligation to conduct a search of material covered by privilege in proceedings in the UK. However, that will only be relevant where all material in a data source is covered by privilege. Where some personal data in a data source are covered by privilege and other data are not, the data controller will have to carry out a proportionate search to find and extract any personal data.

Usually, it will be relatively easy to identify (and therefore exclude) privileged communications with external lawyers. However, the usual difficulties arise with in-house lawyers, who should be as disciplined as possible in preserving privilege in their communications.

Practical guidance for data controllers

The judgments of the Court of Appeal contain practical guidance for data controllers on how to consider the proportionality of responding to a SAR:

- consider carefully what is requested under the SAR, the purposes for which information is sought, the benefits to the data subject of that information and any alternative sources of that information;
- determine what the potential repositories of the data subject's personal data are – where the data is held, in what format and how it can be searched;
- run initial searches to determine the number of 'hits'.

A SENSE OF SCALE

	Reviewed	Disclosed	Cost	
Deer	500,000 emails	63 emails	£116,116	Proportionate
Ezsias	2,400 pages	1,000 pages	Unknown	Proportionate
Candy	17,000 documents	Unknown	£37,000	Proportionate

'the General Data Protection Regulation will be a game changer for data protection when it comes into force in May 2018'

Consider liaising with the data subject at this stage to get agreement on what searches will be done, which keywords used and what reasonable limitations on the scope of the exercise can be agreed;

- evaluate the risk of disclosing information in documents that go beyond the personal data to which the subject is entitled. This information may be commercially sensitive, prejudice the rights of other data subjects or be privileged. Often, data controllers will need to carry out a manual review to extract the personal data and apply the exemptions;
- work out a plan of action for searching, reviewing and extracting the personal data – which sources will be searched, which will not and in what form personal data will be disclosed. Estimate the costs of this exercise – both internal management time and external legal costs;
- document that plan of action.

If the matter goes to court or if a complaint is made to the ICO, the burden of proving that the supply of data would involve disproportionate effort is on the data controller. Data controllers should be prepared to produce witness evidence of what was done and the plan of action will be a key document.

Conclusion

Practitioners will welcome the clarity given by *Dawson-Damer* and *Ittihadieh/Deer*, although that could be short lived – we understand that permission to appeal to the Supreme Court is being sought in *Dawson-Damer.*

Given the emphasis of the court in *Ittihadieh/Deer* on the need to interpret the provisions of the DPA in line with general principles of EU law, we will expect to see more rights-based arguments being employed by data controllers to justify their stance.

The General Data Protection Regulation (2016/679) will be a game changer when it comes into force in May 2018. Although it is unlikely to materially change the right of access for data subjects, the prospect of substantial fines will change the way that many data controllers respond to SARs.

KEY:

Durant	*Durant v Financial Services Authority* [2004] FSR 28
Dawson-Damer	*Dawson-Damer v Taylor Wessing LLP (The Information Commissioner intervening)* [2017] EWCA Civ 74
Ittihadieh/Deer	*Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd & ors; Deer v University of Oxford (The Information Commissioner intervening)* [2017] EWCA Civ 121
DPA	Data Protection Act 1998
YS	*YS v Minister voor Immigratie* [2015] 1 WLR 609
Ezsias	*Ezsias v Welsh Ministers* [2007] All ER (D) 65 (Dec)
SAR code	The ICO's Subject Access Code of Practice
Candy	*Candy v Holyoake and CPC Group Ltd* [2017] EWHC 52 (QB)

Employment Law Clinic

the Speakeasy advice centre

The Cardiff Employment Law pro bono clinic, which has been running in Cardiff since February 2015, is looking for some more volunteer employment solicitors to be added to the rota. Currently, we have nearly 40 solicitors from several firms in Cardiff and the surrounding area, and we hope members of ELA who are based in South Wales would like to get involved.

The clinic runs every other Wednesday, starting at 5.45pm and ending at 8pm. The solicitor will do a brief consultation, take notes and provide advice. Solicitor volunteers need to have 2 years' PQE and 2 years' experience in providing employment advice.

If any solicitors who are based in South Wales are interested, please send an email to info@cardifflawclinic.co.uk.