CLIFFORD

CHANCE

UK: New ICO Guidance on Data Subject Access Requests: Clarity restored?

Data subject access requests (DSAR's) have been a feature of data protection law since the Data Protection Act 1988 and continue to be so. The Information Commissioner's Office (ICO) has just published new detailed guidance on the Right of Access (New Guidance). This replaces the initial ICO guidance of April 2018 and is intended to clarify or assist with issues that organisations have faced in relation to DSARs since then.

Following its consultation on the draft DSAR Guidance the ICO has revised its proposed approach in some regards providing clarity on the three key points:

- stopping the clock for clarification;
- what is a manifestly excessive request; and
- what can be included when charging a fee for excessive, unfounded or repeat requests.

This Briefing explores these areas of the New Guidance in more detail below, and highlights where organisations may wish to consider revising their DSAR policies.

Key issues:

- Timeframe for responding
- Stopping the clock
- Complex requests
- Motive for the DSAR
- What does manifestly unfounded and manifestly excessive mean?
- When can a fee be charged for a DSAR?
- What efforts should be made to find information?
- Information contained in emails

Timeframe for responding to a DSAR:

Stopping the clock

Generally a DSAR should be responded to at the latest within one month of receipt of the request. The one-month time limit can be paused: (i) if there is anything in the DSAR that the data controller requires clarification from the requester on, (ii) if the requester's identification has to be verified; or (iii) prior to receipt of a fee (in the limited circumstances where it is permissible to ask for one)(see further below).

The retention of the 'stop the clock' approach previously endorsed by the ICO under the pre General Data Protection Regulation (GDPR) regime is a welcome change from the draft guidance consulted upon which adopted the approach that the one month clock would continue to run while awaiting receipt of the requested information, fee etc.

The time limit is calculated from the day the DSAR, fee or other requested information is received (whether it is a working day or not) until the corresponding calendar date in the next month.

Although the clock for responding to the DSAR is stopped pending receipt of any clarifying information clarification requests cannot be used as delaying tactic and the ICO expects organisations to:

- contact the individual as quickly as possible (e.g. by phone or email where this is appropriate);
- keep a record of any conversation with the individual about the scope of their request and the date when additional information was sought;
- explain to the individual why further details are being sought;
- be able to justify their position to the ICO, if asked to do so; and
- wait for a reasonable period of time before considering a DSAR 'closed' where there has been no response to a clarification request.

Complex requests

Data controllers can extend the DSAR response time by a further two months, giving three months in total to respond where the request is complex or where a number of requests have been received from the individual relating to the individual's GDPR rights.

If an extension is justified, the data controller must write to the individual within one month of receipt of the request to explain why the extra time is needed. It would appear that non GDPR related requests for information for example litigation disclosure requests do not come within the permitted circumstances for extending the DSAR response time.

The New Guidance sets out seven examples of factors that may add to the complexity of a DSAR, but emphasises that the specific circumstances and the particular request are key to determining whether the request is complex.

One of the listed factors (added following the consultation) is the need to obtain specialist legal advice; however this is qualified by the ICO's view that if a data controller routinely obtains legal advice, a DSAR is unlikely to be complex. For some organisations this may be a somewhat restrictive viewpoint given that the nature of the legal advice sought will be often be fact specific to each DSAR request; particularly in the context of a DSAR made as a prelude to employment disputes and/or other litigation.

Motive for the DSAR

Organisations in the UK are often faced with DSAR's from individuals (often employees in the context of disciplinary or grievance procedures) prior to or upon commencement of litigation against the organisation. The DSAR is used tactically as a pre-disclosure fishing exercise to obtain documents prior to litigation and/or as a form of accelerated disclosure ahead of the court/tribunal disclosure timetable and/or to apply pressure on the organisation to divert time and financial resources away from the litigation to the DSAR exercise. This seems to be a particularly British problem as DSAR's do not appear to be routinely used in this way in other jurisdictions subject to the GDPR .

Prior to the New Guidance, the Court of Appeal reiterated in *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74 that a collateral purpose of the data subject, such as obtaining data for litigation, does not prevent a data controller from dealing with the request. In this matter, Taylor Wessing objected to searching for 30 years of client files, on the grounds that "the supply of such a copy is not possible or would involve disproportionate effort". The Court of Appeal disagreed; Taylor Wessing had taken no steps to identify personal data within its file, meaning that the Court could not assess whether any particular steps would be disproportionate.

In the New Guidance, the ICO has not changed its view that the right to make a DSAR is 'purpose blind' i.e. the purpose for which an individual makes a DSAR does not affect its validity. If the DSAR is clearly a pre-litigation fishing expedition or pressure tactic can an organisation decline to respond on the basis that the DSAR is manifestly unfounded; or manifestly excessive (both grounds upon which a data controller is permitted to refuse to comply with a DSAR)?

What does manifestly unfounded and manifestly excessive mean?

The New Guidance addresses what 'manifestly unfounded' and 'manifestly excessive' mean, but does not address this pre-litigation fishing expedition issue. It clarifies that a request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example where an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption; or
- the individual makes unsubstantiated accusations against an organisation or specific employees which are clearly prompted by malice;
- the individual targets a particular employee against whom they have some personal grudge; or
- different DSARs are systematically sent as part of a campaign, e.g. once a week, with the intention of causing disruption.

The New Guidance emphasises that a DSAR must be considered in the context in which it is made; it is not a simple tick list exercise that automatically means a DSAR is manifestly unfounded if any of the above are satisfied. Although an organisation in the early stages of litigation may well be convinced of the individual's (strategic/tactical) motive(s) for the DSAR (particularly if made by their lawyer) it will be very difficult for the organisation to refuse to respond on the grounds that the individual does not genuinely want to exercise their GDPR rights rendering the DSAR manifestly unfounded. The New Guidance is, however, likely to assist where a data subject is making repeat (e.g. weekly) SARs, designed to ensure that the organisation has to repeatedly expend resources in responding.

The New Guidance considers that a request may be excessive if it is clearly or obviously unreasonable. Organisations are expected to assess whether the request is proportionate when balanced with the burden or costs involved in dealing with the request taking into account all the circumstances of the request, including:

- the nature of the requested information;
- the context of the request, and the relationship between the organisation and the individual;
- whether a refusal to provide the information or even acknowledge if it is held may cause substantive damage to the individual;
- the organisation's available resources (this presumably includes financial, physical and management time resources);
- whether the request largely repeats the substance of previous requests and a reasonable interval has not elapsed; or
- whether it overlaps with other requests (if it relates to a completely separate set of information the New Guidance suggests it is unlikely to be excessive).

Although the expanded clarification is welcome, whether a pre litigation DSAR fishing expedition can be refused on the grounds that it is manifestly excessive because there is insufficient resource to devote to it and the litigation process or because disclosure of broadly the same information will occur in due course is doubtful. It does however suggest that if significant costs will be incurred in responding to the DSAR the DSAR may be considered manifestly excessive.

When can fee be charged for the DSAR?

A reasonable fee can be charged for the administrative costs of complying with a request if: it is manifestly unfounded or excessive (if the alternative option of refusing the DSAR is not exercised); or an individual requests further copies of their data following a request.

The New Guidance expands on what can be taken into account for determining the fee, including the administrative costs of the process of locating, retrieving and extracting information and the staff time taken to deal with the request (charged at a reasonable hourly rate). The latter can be determined by the organisation as there are currently no legislative parameters on the fees for staff time.

Organisation will have to be able to justify the costs charged in the event that an individual complains to the ICO; accordingly it is advisable for organisations to establish an unbiased set of criteria for charging fees. Indeed the ICO expects a copy of the fee criteria to be included in the organisation's' fee request in response to a DSAR considered manifestly unfounded or excessive.

What efforts should be made to find information?

Organisations are expected to 'make reasonable efforts to find and retrieve the requested information'. Whether a search is unreasonable or disproportionate has to be assessed in the context of:

- the circumstances of the request;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

The burden of proof is on an organisation to be able to justify why a search is unreasonable or disproportionate. Documenting the search parameters and the sources searched for the personal data together with the rationale for the approach (technical difficulties, costs, time involved) will all stand an organisation in good stead in the event it has to demonstrate to the ICO that its DSAR response has been reasonable and proportionate.

Organisations are expected to ensure that their information management systems are well-designed and maintained so they can efficiently locate and extract requested information and, where necessary, redact third-party data. The reality for some organisations is that their IT systems are not state of the art and their technology does not necessarily allow for easy searching for personal data, making it a very manual (and expensive) process. Fortunately, the New Guidance is clear that if personal data is deleted by an organisation from its computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean the organisation must go to such efforts to respond to a DSAR.

The ICO will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously ‘deleted’ personal data held in electronic form. It will not require organisations to use time and effort reconstituting information that has been deleted as part of general records management.

CLIFFORD
CHANCE

Information contained in emails

Employers often receive DSARs from (ex) employees asking for all emails held on the organisation's system about them. Where a DSAR is made by a long serving employee this can involve thousands of emails and it is often a very time consuming exercise to address such a request. Helpfully the New Guidance specifically addresses such requests in the following example:

"*An employee makes a SAR for all of the information you hold about them. During your search for their personal data, you find 2000 emails which the employee is copied into as a recipient. Other than their name and email address, the content of the emails does not relate to the employee or contain the employee's personal data*.

You do not have to provide the employee with a copy of each email (with the personal information of third parties redacted). Since the only personal data which relates to them is their name and email address, it is sufficient to advise them that you identified their name and email address on 2000 emails and disclose to them the name contained on those emails, eg John Smith, and the email address contained on those emails, eg JohnSmith@org.co.uk. Alternatively you could provide one email with other details redacted as a sample of the 2000 emails you hold. You should also clearly explain to the individual why this is the only information they are entitled to under the GDPR, but remember to provide them with supplementary information concerning the processing, eg retention periods for the emails.

However, if any of the content within the email relates to the individual, you should provide them with a copy of the email itself, redacted if necessary."

Given that one of the objectives of a potential claimant is often to obtain copies of emails using a DSAR (i.e. advance disclosure), practically, providing only confirmation of the volumes of emails and one example, removes some of the incentive for claimants to make such requests in the first place.

The New Guidance addresses many other aspects of DSAR's which are not covered in this Briefing; your usual Clifford Chance contact would be happy to advise you further.

The New Guidance can be accessed here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

CONTACTS

Michael Crossan
Partner
London

T +44 (0)20 7006 8286
E michael.crossan@cliffordchance.com

Chinwe Odimba-Chapman
Partner
London

T +44 (0)20 7006 2406
E chinwe.odimba-chapman@cliffordchance.com

Alistair Woodland
Partner
London

T +44 (0)20 7006 8936
E alistair.woodland@cliffordchance.com

Kate Scott
Partner
London

T +44 (0)20 7006 4442
E kate.scott@cliffordchance.com

Tania Stevenson
Knowledge Director
London

T +44 (0)20 7006 8938
E tania.stevenson@cliffordchance.com