LINEAL

DATA SUBJECT ACCESS REQUESTS:

USING EDISCOVERY TOOLS TO ENSURE COMPLIANCE AND SAVE COSTS

DATA SUBJECT ACCESS REQUESTS

> IT IS WORTHWHILE TO UNDERSTAND HOW eDISCOVERY TOOLS CAN BE USED TO DEAL WITH DSARS, PARTICULARLY IN CASES INVOLVING "BIG DATA". THIS PAPER AIMS TO OFFER PRACTICAL GUIDANCE IN THAT REGARD AND WILL SHOW HOW ORGANISATIONS CAN MINIMISE ANY COST AND DISRUPTION CAUSED TO THEIR BUSINESS BY DSARS.

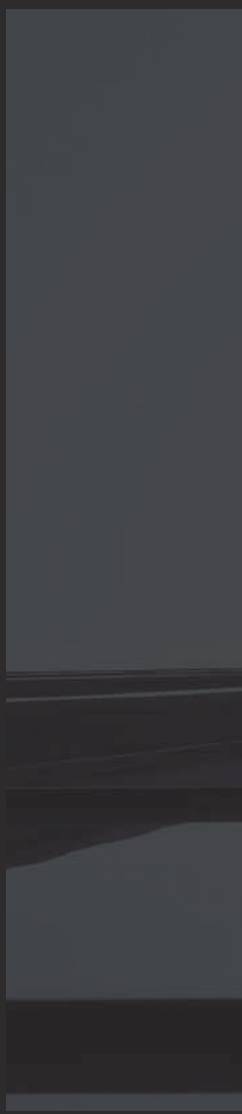
INTRO

USING eDISCOVERY TOOLS TO ENSURE COMPLIANCE AND SAVE COSTS

Among the remarkable developments of our time is the huge increase in data volumes. It is estimated that by the year 2020, about 1.7 megabytes of new information will be created every second for every person on earth. Other statistics are equally astounding. Businesses of all sizes will require some kind of data analysis system in the not-too distant future.

Meanwhile, in the legal realm, Data Subject Access Requests (DSARs) are becoming more common. Individuals are now more aware of their right to request personal data and will robustly exercise that right, whether out of concern for their own privacy or as a means of seeking an edge in litigation. Indeed, it is often the official policy of data protection authorities to raise the public's awareness of these rights.[1]

Given these developments, it is worthwhile to understand how eDiscovery tools can be used to deal with DSARs, particularly in cases involving "big data". This paper aims to offer practical guidance in that regard and will show how organisations can minimise any cost and disruption caused to their business by DSARs.



A SHORT REFRESHER ON DSARs

The DSAR regime is intended to provide transparency to individuals in respect of their "personal data"[2] held by an organisation. Often the organisation is the individual's current or former employer but it can also be, for example, a retailer or an academic institution.

Under the General Data Protection Regulation (GDPR) which came into force on 25 May 2018, data subjects are provided certain rights in relation to their personal data held by an organisation.

Article 15 of the GDPR states that a data subject has the right to confirmation from a data controller whether or not their data has been processed and if so:

- Where the information on the data subject has been sourced from if it was not collected from the data subject
- The reason for the processing
- Who the data has been disclosed to
- The existence of automated decision-making, including profiling
- The categories of personal data processed
- How long the data will be stored for

1. Data protection rights: What the public want and what the public want from Data Protection Authorities (Information Commissioner's Office report, 2015). Available here.

2. NB: the mere fact that an individual is named in a document does not mean that the entire document is the individual's personal data. Personal data has to be "biographical in a significant sense" and the individual making the request has to be the focus of the information: Durant v FSA [2003] EWCA Civ 1746.

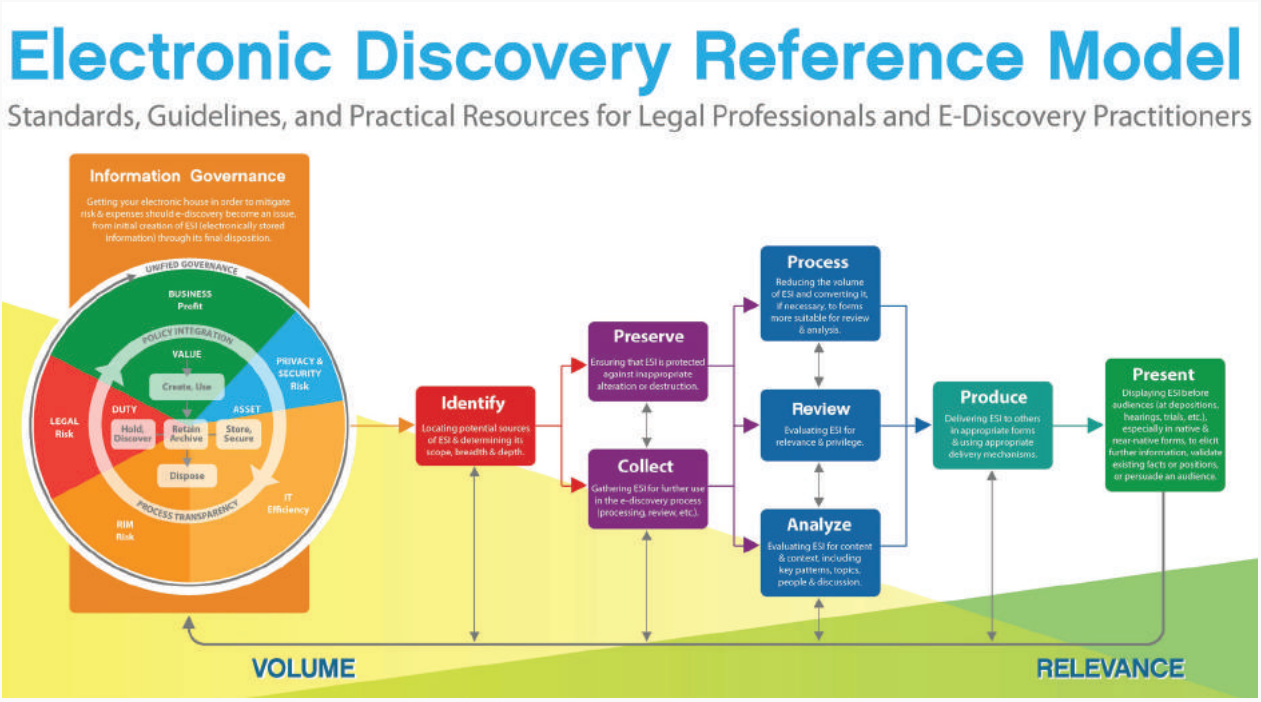
This paper aims to offer practical guidance in that regard and will show how organisations can minimise any cost and disruption caused to their business by DSARs.

DSARs present a number of risks to organisations. As with disclosure in civil litigation, the most obvious risk is that DSARs can reveal material that is damaging to the organisation's position. However, a DSAR can also reveal a cause of action in its own right, e.g. unlawful or unfair processing. From a practical standpoint, there is also the risk of added cost and inconvenience if the individual is not satisfied with the extent of the DSAR response and asks for better compliance.

Under Article 12(3) of the GDPR, an organisation has one month to comply with a DSAR. It is not permissible to charge a fee or refuse the DSAR unless the request is "manifestly unfounded or excessive, taking into account whether the request is repetitive in nature". Given these provisions, the need to limit the time and money spent dealing with DSARs is crucial.

USING THE EDRM TO DEAL WITH DSARs

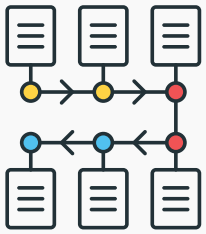
The Electronic Discovery Reference Model (EDRM) is useful as a general guide when responding to DSARs involving electronic data.



Depending on the nature of the case, certain stages in the EDRM may need to be repeated. It may even be that more than one EDRM workflow will need to be run simultaneously, e.g. if data is stored in multiple locations. As we move through the EDRM from left to right, the overall *volume* of data being handled (shown in yellow) should decrease, but the volume of *relevant* data identified (shown in green) should increase. Let us take a look at the different stages of the EDRM workflow and how they relate to DSARs.

INFORMATION GOVERNANCE

Information governance refers to the systems and procedures that you (or your client) have in place to manage electronic data. At this stage, you should try and get a general understanding of what data the organisation holds, how and where the data is stored and how it is organised. Ascertain, for example, whether there is only one email server and whether there are backup systems that can be used to recover any deleted data. You may need to review the organisation's written plans or policies, and/or speak with the IT team.



It may become apparent to you at the Information Governance stage that improvements need to be made to mitigate certain risks in the future (e.g. privacy breaches, unlawful processing of personal data). Forensic experts and data protection lawyers can assist with this.

IDENTIFICATION

Identification is the next stage. This is a narrower enquiry that involves identifying the general classes and sources of data that may be responsive to the DSAR. Note that we are still "scoping" at this stage; we are not yet handling data.

Start drawing up a plan that incorporates answers to the following:

- Which individuals' data (i.e. "custodians") within the organisation should you focus on, and which can you disregard? The DSAR subject's own PC and email account should obviously be targeted, but you should also think about which other people may hold responsive data – e.g. the individual's manager and team members, as well as departments such as HR, accounts and legal.

- Which devices and networks should you target? Email servers are good places to start, but bear in mind that data is increasingly being stored in smartphones, tablets, cloud servers and elsewhere. It is also important not to overlook "structured" data, such as that found CRMs and accounting software.

- Have you overlooked any hardcopy documents relating to the individual? Think about things like HR files and any of the individual's personal files or notes. (Hardcopy documents can later be converted to electronic form to streamline the review.)

PRESERVATION AND COLLECTION

Preservation and collection can in some cases be sequential steps, but usually they are interrelated and occur simultaneously. These are the stages where you start to handle actual data. Your choice of data collection method(s) – and by extension preservation – will depend on the circumstances on the case.

It may in some cases be sufficient simply to hand over an external hard drive to an eDiscovery service provider. In other cases, it is advisable to engage a forensics expert who can either conduct searches of the data on site or take copies of the relevant devices for further analysis.

PROCESSING, REVIEW AND ANALYSIS

Processing, Review and Analysis are where the bulk of the work takes place, and should involve the uploading of the data onto an eDiscovery platform such as Relativity or Clearwell. There are several advantages to doing this:

- eDiscovery platforms have a variety of search tools an–d filters for interrogating the data. Searches and filters can be based on date ranges, file types, keywords and numerous other properties and they are compatible with Boolean operators.

- *Early Case Assessment (ECA)* tools include a range of visual and statistical features that can identify general trends in the data – for example, which people within the organisation hold the most data containing relevant search terms, and which periods of time appear to be the most crucial. This can, in turn, save you time or help you refine your overall approach. You may decide, following your use of ECA tools, to revise your findings from the Identification stage or to prioritise certain custodians or devices over others.

- With the assistance of these search and ECA tools, you will be able to narrow your target data significantly and then assign "batches" to people within your team for document review. If your in-house resources are insufficient, you can engage document review lawyers or paralegals on a temporary basis. Setting up and training reviewers on an eDiscovery platform is quick and easy, and there are user-friendly tools for assigning batches and setting up quality control processes.

- eDiscovery platforms allow reviewers to code documents according to customisable criteria. In an DSAR case you may, for example, want to code documents as responsive or not responsive, privileged or not privileged, and also flag them as relating to certain factual or legal issues (e.g. "unfair dismissal", "discrimination"). You will be able to isolate documents that require redaction and then use the available redaction tools to remove references to third parties and other non-disclosable information. (Redactions are permissible under the DPA, provided that the personal data is disclosed in an "intelligible form".)

- *The Analytics* features of eDiscovery platforms can save significant time and expense in document review. There are many tools that fall under the Analytics umbrella, but here are some examples:

- *Structured Analytics* can speed up a review by arranging the documents better – for example, email threading can organise long email chains in a more logical way so that reviewers can work through them more quickly.

- *Predictive Analytics* uses advanced algorithms to make predictions about whether certain documents will be relevant, based on "sample" sets which have already been reviewed and coded. Predictive coding is useful in cases involving very large volumes of data, where it is not practicable to review all documents manually. Case studies have repeatedly found predictive coding to be no less accurate than manual review, and its use has been approved by the courts.

PRODUCTION & PRESENTATION

Production, followed by Presentation, refer to the handing over of the data that you have identified as responsive. These steps can be completed easily and inexpensively with an eDiscovery platform.

CONCLUSION

If your organisation has been served with an DSAR, you will want to ensure that your response is not only compliant (i.e. it discloses everything that is required under the GDPR and no more), but also defensible (i.e. your methodology is justifiable in the event of a legal challenge). In the likely event that you are dealing with electronic data, the most practical and cost-effective way to do this is to use an eDiscovery platform, with the EDRM as your general guide to the process.

PRACTICAL TIPS FOR COMPLYING WITH DSARs

- *Diarise the time limit for compliance with the DSAR (currently one month), and keep your resourcing under review as the project progresses. It can also help to diarise earlier milestones – for example, target dates for completing the review of different "tranches" of documents and target dates for completing different stages of the EDRM.*
- *As you work through the EDRM, try and identify ways to improve your organisation's information governance for future cases (see further tips below).*
- *Keep a record of the documents you disclose, including (if applicable) a detailed methodology setting out what search terms you used, how you filtered data and what redactions you applied. (An eDiscovery platform can save and reproduce these records quite easily.) This can be useful if the individual raises a challenge in the future.*
- *If necessary, seek specialist advice from an eDiscovery service provider or lawyer (or both).*

For managing your organisation's data generally:

- *Ensure that the data mapping policies and procedures your organisation implemented as part of its GDPR compliance preparation is kept up-to-date and reviewed regularly.*
- *Implement document destruction policies. Obviously, you should not destroy potentially responsive data after receiving a DSAR (or any other kind of disclosure request), but the GDPR provides that a controller should not keep personal data for longer than it is required. If you do retain data, make sure you have a policy relating to data retention and can justify why particular data is being kept by your organisation.*

LINEAL

We assist businesses with identifying a tailored solution to their needs and help them navigate the complexities involved when law, technology data and compliance meet.

SERVICES

Digital Forensics
Cyber Security
eDiscovery

LINEAL

125 Finsbury Pavement, London, EC2A 1NQ
+44 (0)20 7940 4799
www.linealservices.com

Let us tell you more about the amazing things we do.

info@linealservices.com