Bird & Bird

Privacy Unpacked – Episode 3

Podcast transcript – Mastering DSARs: Handling Data Subject Access Requests in the UK and Europe

Featuring Vincent Rezzouk-Hammachi (Partner, International Privacy & Data Protection practice) and Laura Goold (Associate, International Privacy & Data Protection practice)

October 2023

Vincent Rezzouk-Hammachi:

Welcome to our third episode of Privacy Unpacked from Bird & Bird. I'm Vincent Rezzouk-Hammachi, a partner in our London office, looking after Bird & Bird's Privacy Solutions service line within the privacy and data protection team. In this episode, our team will be discussing rights of access, or as they are more commonly known in the privacy world, DSARs.

I am joined by one of my colleagues, who has worked on a variety of DSARs for the last 5 years, Laura Goold, who is an associate in our London team.

Laura Goold:

Hello.

Vincent Rezzouk-Hammachi:

Today we are going to provide an overview of DSARs in the UK and Europe, with a particular focus on how we handle them in the UK. Before we get into that, Laura, what would you say are the most common types of DSAR?

Laura Goold:

Thanks, Vincent. So, in my experience, most DSARs fall into 2 self-explanatory buckets. Consumer and employee DSARS. Now, although the law governing these is the same, in practice handling the two is quite different. So at Bird & Bird we tend to be more involved with employee DSARs, due to the complexities and volume of data associated with them. But in reality, most clients receive far more consumer DSARS.

Vincent Rezzouk-Hammachi:

We'll come back to employee DSARs in a minute, but it's very interesting to hear that there are more consumer DSARs. Do you have any idea of the volume of these, and why it's so high?

Laura Goold:

So, the volume of consumer DSARs tends to vary based on the industry with banks, utilities and retail companies typically receiving the highest volumes. And often these can be as high as a couple of thousand per month, so many controllers have automated their responses and implemented self-service portals to lessen the

burden. This works well if the DSARs are process-driven and the level of data held about individuals is low.

It's much more challenging when the data held about an individual is complex, so for example if they have on-going complaints. It's also worth noting that certain events can cause a surge in consumer DSARs such as large data breaches. So, if you're receiving publicity over enforcement action, you should prepare for a deluge of DSARs.

So I mentioned self-service portals, but controllers do still receive DSARs via email, especially where an email address is listed in the privacy policy. Now most of these emails a very similar, as they've been sent or generated by platforms. However, organisations should note that any form of DSAR is valid. In theory, customers can ask for their data on Facebook if they want.

Vincent Rezzouk-Hammachi:

How can you tell that they've been sent by platforms, and how does it change the way you handle them?

Laura Goold:

Yeah, so there are actually two types of what I call platform DSARs: those sent by the individual's email account, and those sent from the platform itself. So the first category usually all look alike. They use template wording, include a reference number and often at the end of the email say which platform was used. These emails are sent by the individual signing up to a service such as Mine and PrivacyHawk, and the individuals grant the platform access to their inbox, and it scans it to see which companies it communicated with the individual to see who is likely processing personal data about that person.

So for these DSARS, you can ignore the fact that it was sent using a platform, they are valid and you would need to follow your usual process. Now the other category of platform DSARs are usually sent by a generic email address owned by the platform. They're instantly recognisable as they will include branding and will tend to ask you to log in to the platform to view the DSAR.

Vincent Rezzouk-Hammachi:

And the second one, should companies really access the link that could be a security risk as it sounds like a phishing email?

Laura Goold:

Yeah that's a good point. They usually are actually quite safe and quite legitimate but you don't need to log on to the platforms. We have quite clear guidance from the ICO that if the details needed for you to be able to respond to the DSAR are locked behind a platform, then the DSAR has not been validly made. If the details are included in the email notification, then it is still a valid DSAR. There will just be a question of whether the platform has authority to make the DSAR on behalf of the individual. But for that, companies should follow their standard policy when dealing with DSARs made by agents or authorised representatives.

Vincent Rezzouk-Hammachi:

That makes life a bit easier I suppose, but I'm sure that position varies across Europe. Let's turn back to employee DSARs, since they sound pretty meaty. When do you usually see them?

Laura Goold:

Yeah, so often the employee DSARs I see have been made whilst the data subject is going through a grievance or disciplinary proceeding, or they've been sacked, or there's a redundancy process going on. We also occasionally see them from unsuccessful applicants.

Vincent Rezzouk-Hammachi:

It must be quite concerning for clients to receive DSARs when they've got disciplinary proceedings going on, or from ex-employees, as surely they are being used as a phishing expedition. Do clients still need to respond to these DSARs?

Laura Goold:

Yeah, so, it often feels like a phishing expedition, especially for ex-employees where it almost feels like pre-action disclosure. However, that doesn't really matter. For the most part, the motive behind the DSAR doesn't matter. So the two exemptions which allow you to not fulfil a DSAR are where it is manifestly unfounded or excessive. These exemptions are very narrow.

Vincent Rezzouk-Hammachi:

You said exemptions are narrow. Can you summarise the position on each as I am sure our listeners are curious as to when these apply?

Laura Goold:

Sure. I'm going to focus on the UK position given that's what I know best, so the interpretation may

vary in the EU. So starting with manifestly unfounded. To fall under manifestly unfounded there needs to be either no intention to exercise the right of access, or the DSAR is being used maliciously to harass and disrupt the controller.

For the first point, this has to be very obvious. We're talking along the lines of the individual actually saying they'll withdraw the DSAR if the controller pays them, or they get something else in return. For the second option, again, this is quite a high bar that requires a degree of obviousness. Most DSARs feel like they're being done to cause disruption but this isn't enough. Usually, we'd look for something in the original request itself, or other communications with the data subject, that show clear malicious intent. For example, they say they are doing it to make the controller pay, or they're making unsubstantiated allegations against a particular individual employee at the controller.

But this all needs to be in the face of the DSAR. It's not permitted to ask someone why they're making the DSAR, so then the other exemption, manifestly excessive. Based on ICO and EDPV guidance, this only applies where a data subject has made multiple overlapping requests during a continuous period of time. Controllers can't rely on this exemption where they have received a large number of requests all from different data subjects. The point here is that it has to be from the same person.

Vincent Rezzouk-Hammachi:

OK so, like you said, both exemptions seem very narrow. Now, let's say I'm a data controller, and I decide to rely on one of the exemptions. Do I still need to reply to the data subject?

Laura Goold:

Yeah, this is an important point. So you would need to inform the data subject why you're not fulfilling their DSAR, and the reasons why. This should be done as soon as possible, but at the latest within a month of receiving the DSAR.

Vincent Rezzouk-Hammachi:

OK. Now, say you receive the DSAR, and decided that it's valid, and you can't rely on an exemption. What would be the next step; what should we do?

Laura Goold:

So firstly, I would work out the deadline, and get that diarised, as it can be quite easy to miss it. So the deadline is one month from receipt of the DSAR. You can extend this by two months where the request is complex, or the individual has made multiple requests at the same time. Now these multiple requests don't necessarily all have to be DSARs, they could be requests to exercise other rights. Just make sure to inform the data subject if you're exercising the extension. And the other point to flag, on the deadline, is that this only starts once you have enough information to actually action the DSAR.

So you need to be confident in the requestor's identity, and if they're acting on someone else's behalf that they have the correct authority to do so. You might also need to clarify the scope of the request, so for example, if you need to clarify the scope of the DSAR with the individual to check what they actually want, before you can comply, then the deadline will be calculated from when they supply this information. But if you're doing this, you need to be careful. You can't just run the clock out and then ask for the clarification. You should be asking for this information as soon as is reasonably possible.

Vincent Rezzouk-Hammachi:

Yes, timings are very important indeed. I know from my experience actually that many data subjects will follow up when it gets close to the deadline. Now you know how long you have to comply with a DSAR, how do you actually go about fulfilling a DSAR?

Laura Goold:

Next is locating the data. So in my opinion, this is the most important part of the DSAR. We have some pre-GDPR cases in the UK focussing on searches and how far you have to go. So controllers absolutely must run searches and should do so at an early stage to determine the volume of data and the resources needed to review it.

The main sources of data are emails and other communication such as chatbots and instant messages, and in company-specific systems such as payroll and HRIS systems for employees and customer databases where dealing with consumers. So increasingly, we're starting to see individuals ask for information contained in WhatsApp messages and similar. This can be valid if you, as an employer are directing staff to use third-party tools, or are at least aware or and condoning such use for work purposes.

This will be considered to be under your control. This is similarly true if you allow some staff members to conduct their work from personal

email accounts or personal mobile devices. So you won't typically be able to access this information centrally, like you would for employee email. In this case, usually you will need to ask individuals to provide you with copies of messages in scope and ensure they carry out an appropriate search.

It's important for this last point to remember that in the UK, it is a criminal offence, to prevent disclosure of data that ought to be disclosed under a DSAR unless you can show you held a reasonable belief that this could be withheld and this carries personal liability. Searching can be an onerous task. The obligation isn't to leave no stone unturned, but to perform a proportionate search. Recent ICO guidance from employers has emphasised proportionality is a relevant consideration although EDPB guidance appears to claim that proportionality is a relevant consideration or they there is no such limit in the wider EU.

Certainly at present, certain employee DSARs have still been primarily based in the UK despite this guidance. Part of the problem is that the case load discussing proportionality is limited and the only case in the UK that discussed costs pre-GDPR only acknowledged that £100,000 was not proportionate. Certainly clients want to spend a lot less than this. So we often get asked to provide advice on how to tailor search terms, and this can be quite case-specific to the nature of the client's IT set-up.

Vincent Rezzouk-Hammachi:

Great! So, I've sorted out my deadline, and now my search is quite early in the process, as I want to have plenty of time for the review. So, what do I need to do in the review?

Laura Goold:

This is where the bulk of your time and money will go. I'll walk you through how I tend to handle the review, as this is what I've found works best for me but I know some people prefer a different approach.

First, I avoid having to review documents on paper or on my desktop in email or PDF form. Instead, I ask our wonderful forensic services team to process the data and upload it to our e-discovery platform. I do this as we can refine the data more by duping it and by threading conversations to keep things together. I also find the review to be a lot quicker, as it's easier to navigate between documents, and then, within the documents you can jump to where the key words appear. Now, I appreciate using forensic services may not be an option for everyone but I really recommend doing so for bigger DSARs. For DSARs of under, say, 500 documents it might not be practical, but most employee DSARs will exceed this number quite quickly and the costs of using e-discovery platforms here are often readily saved as compared to the human cost of the review, and the assistance they provide in keeping an audit trail of decisions taken on documents. When we're using these documents, we tag documents to flag which can be disclosed for all, which contain no data and which need to have some data either extracted or redacted. We can also flag exemptions such as privilege and documents which fall outside of scope, either of specific search criteria or which duplicate existing data. When we're done, we can then pull these into document sets that can be disclosed.

Vincent Rezzouk-Hammachi:

Great! So, what does the outlook of this look like? You mentioned extraction, so what does the requestor receive?

Laura Goold:

So yeah, there are two approaches to responding to a DSAR. Redaction and extraction. So redaction is your traditional black line approach, where you black out parts of documents that should not be disclosed.

Extraction is our preferred approach, and we have seen it accepted by the ICO and DPC, and I'm sure other DPAs like it. In the UK, we have a key pre-GDPR case which states data subjects are entitled to data, not documents. And the CJEU has also stated in a more recent case this year that, provided the approach to disclosure gives the data subject enough context to understand their data, this should be sufficient.

So this means, with extraction, we provide the snippets that consist of personal data, rather than blackline copies of documents that had contained personal data. So I know this sounds quite abstract, but in practice it would look more focused, and it also means data subjects do not have their data buried in pages of blacked out text. So, with the snippets or the extractions, we put these into a date-ordered table that's shared with the data subject. In the table, we keep email chains and message conversations together for readability. Along with the table, we also provide a PDF containing all documents that could be disclosed in full, and this is usually things like payslips and appraisals.

Vincent Rezzouk-Hammachi:

Thanks Laura, sounds like a pretty intense process overall. And you still need to draft a cover letter, setting out all the required information of Article 51 of the GDPR. Do you have any top tips for the controllers that you want to share about this?

Laura Goold:

Yeah I'd agree, the reviews are quite time-consuming and high-pressured. So first, ensure all teams that may receive DSARs pass them on promptly, as the clock starts as soon as someone in the business receives a DSAR. So for example, make sure customer services knows to route DSARs to the privacy team. Two, run searches at an early stage. The reviews take up time, and throwing more people at them doesn't always help. And three, never let the senders or recipients of the emails that are subject to the review, redact or extract their own emails. It's not particularly professional, and you'd also be disclosing the fact that the requester has made a DSAR to those people.

Vincent Rezzouk-Hammachi:

Thank you so much for joining us today on that run-through on responding to DSARs. We hope you found this episode of Privacy Impact useful. If you have questions for one of our team members, or any suggestions for future episodes, please do get in touch. We look forward to you joining us next time.

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw