The Work Couch

Navigating today's tricky people challenges to create tomorrow's sustainable workplaces

RPC

Season 3

Episode 4 – Data protection and HR-related challenges (Part 2), with Jon Bartley and Helen Yost

Ellie: Hi and welcome to the Work Couch Podcast, your fortnightly deep dive into all things employment. Brought to you by the award-winning employment team at law firm RPC, we discuss the whole spectrum of employment law with the emphasis firmly on people. Every other week we unpack those thorny HR issues that people teams and in-house counsel face today and we discuss the practical ways to tackle them. My name is Ellie Gelder, I'm a Senior Editor in the Employment, Engagement and Equality team here at RPC and I'll be your host as we explore the constantly evolving and consistently challenging world of employment law and all the curveballs that it brings to businesses today. We hope by the end of the podcast that you'll feel better placed to respond to these people challenges in a practical, commercial and inclusive way.

Today, in the second part of our discussion on data protection and HR related challenges , I'm thrilled to be joined once again by two experts in this field, Jon Bartley, partner, and Helen Yost, senior associate.

Jon and Helen both work in our data and privacy team, with whom our employment lawyers work very closely to seamlessly support our clients' employment law and data protection compliance, which are often connected, as we will find out shortly.

So a very warm welcome back to both of you, thank you for being here!

Jon: Hi Ellie, nice to be here.

Helen: Thanks, Ellie.

Ellie: Helen, you both mentioned in part 1 last time a particularly knotty area, which is data subject access requests so please can you explain why these can be so problematic for employers?

Helen: Yes, as Jon said, these kinds of requests can cause a lot of pain for employers just because of the resources and time needed to deal with them. A very common issue faced by our clients is the problem of having to find and sift huge volumes of data. If you can imagine, if you have a long-standing employee who makes a subject access request, you may hold a huge amount of data on that individual, not just indeed from emails sent to and from that person in the course of their employment. And often this is just the volume and scale of SARS can be beyond the scope of in-house teams to deal with. And you need to be able to take that huge data set, identify first of all, identify the relevant data on your systems, extract the relevant data, distinguish personal from business data, de-duplicate, find, you know, take out duplicates of the same email threads, apply appropriate redactions and the application of exemptions. And all of this while meeting a tight deadline of one month, which can sometimes in some circumstances be extended by an additional two months, but that's a very short time in which to deal with that amount of data. As Jon said earlier, we can assist with dealing with these sorts of subject access requests. We have e-discovery tools which can automate a lot of this sifting of data and finding the relevant documents. But this is a big issue for clients currently.

Another issue that crops up quite often are where privacy notices are either not up to date or don't comply completely with data protection law or sometimes not in place at all. And this is an issue because it's often forgotten about actually, but as part of a subject access request, along with the data that you have to provide, you also have to give the data subject certain privacy information, which is typically included in a privacy notice. So if you don't have a privacy notice, there's then additional time taken to sort of put together and provide the privacy information that you're required to provide. Another issue we're finding actually increasingly is requests for information from people's phones and personal devices, particularly in relating in relation to messaging services. And a problem that our clients often grapple with is working out whether that information, those messages on devices are within scope of the SAR and whether they need to be searched and requested. So yes, as we mentioned earlier, we will discuss this in more detail in a future Work Couch episode.

Ellie: And Helen, our employment lawyers have also spoken on previous episodes about the real headaches that you've just outlined can crop up when it comes to these subject access requests. For example, when they arise during a redundancy

process, because that can then really cause severe delays to that process. So how should employers navigate these situations effectively?

Helen: Yes, they are difficult. It's important that employers realise that you're not actually permitted to look behind at the purpose or the reason why the person is making a subject access request. You must deal with it regardless of the motive or the reason. Having said that, you can by law request or ask the requester to narrow the scope of their SAR. So for example, if they've made a request for all of their data, you can ask if there's a particular set of documents or information relating to a particular period of employment or incident that they are interested in receiving from you. And this can really help actually both sides to really focus efforts on finding the information that they are interested in receiving. However, if the person isn't willing to do that and is clear they want to receive all of their data, then you must proceed to deal with it as they've requested. It's important to remember, I think, that it's a right to personal data not to information or documents, and not to general information of the business. However, in practice, it can sometimes be quite challenging to make the distinction and apply appropriate redactions and know which documents you should provide and which ones you shouldn't. But I think if you keep in your head that you're providing the request to his personal data, not anyone else's and not business information as such, that can really help steer you along the right path. And then once you've identified the data that's relevant to the request, remember to consider what exemptions from a disclosure may apply to that personal data set. For example, the one for legally privileged information or for third party data.

Ellie: Thank you, Helen, that's really helpful. Jon, can you just summarise for us the potential consequences of getting data protection wrong?

Jon: Yeah, sure. So I guess the main consequence that most people are aware of is the potential for regulatory fines. And since 2018, the maximum fines are 17 and a half million pounds or 4 % of global turnover, whichever is greater. These are significant amounts of money, you'd expect, particularly with bigger companies. But it's fair to say that in the UK, we don't really have a history of fines at that level. The multi-million-pound fines, and we've had a few in the UK, but they've been mainly reserved for major security breaches. But most of our clients operate across both the UK and the EU. And the national authorities in the EU, certainly in recent years, have been much more robust in imposing significant fines in the tens of millions or hundreds of millions for non-compliance with GDPR.

So that's, that's fines. I mean that's the one that everybody's kind of aware of and is trying to, trying to avoid. However, sometimes a bigger and a more costly consequence than fines can be the need to completely shut down a data processing operation and transition to something completely different and potentially delete all the data that was collected through that non-compliant process. That can often lead to a bigger business impact than any fines in terms of the expense and the impact on your business ops. You know particularly if it's, for example, customer data that you've accrued that has delivered quite a lot of intelligence to the business, which you then have to completely delete and start from scratch. There's also the risk of having to defend and potentially settle civil claims from affected data subjects who might bring either large claims on their own or might be a number of people bringing smaller claims that causes a lot of pain for the business. And of course there's reputational impact and the impact on your brand, particularly if that breach affected customer data that can really have an impact on market share.

Ellie: So a whole range really then of quite damaging implications for getting it wrong. Can you just run us through your top tips, Jon, for avoiding those worst consequences?

Jon: Well, the main tip, I think, is to ensure that within your business, you establish and maintain a robust culture of respect for privacy and that you have a sort of a governance architecture that supports and reinforces that culture. You know, you don't want everyone in the business to be an expert on this stuff, but you do want them to have an antenna for what's okay, what might not be okay, and to encourage reporting of concerns up the line. So, building appropriate channels for this within key functions like HR and say marketing, you know, and having data champions in those teams who are well trained on the issues and trained to look out for them will really help with that. You know, you need some eyes and ears on the ground outside of the data compliance or the legal team or whoever is ultimately responsible, maybe the data protection officer, so that they are more likely to hear about the potential problems before they arise because they've got champions around the business looking out for them. and ideally, you're having sort of fairly regular meetings to discuss what's coming up in the pipeline. Is there going to be an investment in some new HR software that's being proposed? You know, if that's communicated early on, it can have a massive difference to, know, whether or not you do it. If you do it, how you configure it and all of these things, which can be quite hard to reverse engineer if they're dealt with too late. Similarly with things like vendor negotiations on the contract, vendor due diligence. You know, you want to do all, you want to capture all of this early to give yourself the best possible opportunity to deal with any potential risk. And as part of your overall governance structure, you need to have a process for screening some of these new initiatives to see whether you need to do a risk assessment, an impact assessment, and making sure that they're properly done. Now, assuming you have a governance structure that's already in place, one thing I would say is that with the advent of AI, now

is your time to be reviewing and upgrading your governance processes to take account of the broader risks that AI brings. So not just from things like the EU AI Act, which imposes specific obligations and restrictions on particular use cases for AI. But there is legislation increasingly in various jurisdictions around the world now, which are specifically going after AI, not just from a privacy perspective, but slightly more broadly.

And having that baked into your governance structure for new things you want to onboard is important. Another tip is I would say, apply the smell test. You know, would this activity be considered intrusive by your staff? Is there another way we could achieve this objective that would be less intrusive? And could we offer that as an option? Would our employees expect us to be doing this? Are they going to be made aware of it? You know, these sort of common-sense questions that you just ask without any huge knowledge of law can actually go quite a long way in getting to the right answer. And it's also worth mentioning that this year, during 2025, the ICO is updating its guidance on various data protection and employment topics, such as recruitment and employment records and things. So I would recommend that HR professionals who have an interest in this do keep an eye out for those drafts when they're released.

Ellie: And finally Helen, what is on the horizon for data protection and what key pieces of information can help guide employers in this area?

Helen: Well, there's some new data law coming soon in the UK. The Data Use and Access Bill is currently making its way through Parliament. It's not a wholesale change to the existing UK GDPR regime, but it does make some changes to UK data protection law, including some that are relevant to employers, including some new rules on subject access requests and automated decision making and changes to what is considered a, can be considered a legitimate interest for processing personal data. Looking beyond our shores, there is of course the EU's AI Act. Now this is not a UK law, it's an EU law, but lots of our clients will be caught and there are things that they will need to think about before rolling out AI. There are some AI uses that will be strictly prohibited. For example, in the employment context, AI used for emotion recognition in the workplace and there are some high-risk processing activities which will be subject to quite strict controls. AI, it's a really hot topic at the moment, lots of discussion, still to play out on it and both the UK and EU regulators are rolling out guidance and commentary on how to ensure data protection compliance when using AI. One of these actually is the DSIT, the Department for Science Innovation and Technology, which is carrying out a consultation on its self-assessment tool, AI Management Essentials. AI Management Essentials is a self-assessment tool that DSIT has designed to help businesses put in place appropriate management practices for the development and use of AI systems, which will be a useful addition to some of the issues and things that Jon was talking about earlier about governance and appropriate governance within companies. It is designed for SMEs and startups, but it can be useful for larger organisations and indeed sort of divisions of large organisations that are proposing to use AI and thinking about how to put in place the right structures to support that use. And of course, it may be of assistance, you know, thinking, you know, what we're talking about today to companies looking to roll out AI recruitment tools. As Jon mentioned, the ICO is producing a lot of guidance on various areas relating to employment and data protection and indeed on lots of other issues relating to data protection. Jon mentioned some of the useful guidance that's coming down the tracks. I think as a good general tip, just checking the ICO's website, it's a very good place to start for guidance on particular issues. For example, it has some good tips and practical guidance on how to deal with subject access requests. It has some template transfer risk assessments and advice on direct marketing. So it's a very good place to start if you're grappling with an issue to do with data protection.

Ellie: Well, thank you so much Helen and Jon. You've both outlined some really fundamental areas that employers really need to be alive to when it comes to data protection of their workers. And you've given us some really helpful practical tips to navigate those. And you set us up perfectly for our future Deep Dive episodes. So we look forward to talking to you again soon.

Jon: Thank you very much for having us, Ellie. It's been a real pleasure. And yeah, we look forward to returning to the Work Couch soon to talk about this in more detail. And in the meantime, and maybe we could include this in the show notes, your listeners may wish to subscribe to our Data Dispatch, our monthly newsletter that Helen referred to earlier, which is our monthly summary of all the latest developments.

Ellie: Absolutely, thank you Jon. Yes, we certainly will include a link to that one.

Ellie: If you would like to revisit anything we discussed today, you can access transcripts of every episode of The Work Couch podcast by going to our website: www.rpclegal.com/theworkcouch. Or, if you have questions for me or any of our speakers, or perhaps suggestions of topics you would like us to cover on a future episode of The Work Couch, please get in touch by emailing us at theworkcouch@rpclegal.com – we would love to hear from you.

Thank you all for listening and we hope you'll join us again in two weeks' time.

And to make sure you don't miss any of our fortnightly episodes please do hit the like and follow button and share with a colleague.