The Work Couch

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

RPC

Season 3

Episode 2 – Data protection and HR related challenges (Part 1) 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.

In today's episode, we're discussing the topic of data protection and some of the HR related challenges that can often crop up. Joining me today, in part 1 of our two-part series, are two experts in this field, Jon Bartley, partner, and Helen Yost, senior associate, who both work in our data and privacy team and 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 to both of you. It's wonderful to have you today.

Jon: Hi Ellie, nice to be here.

Helen: Thanks, Ellie.

Ellie: So just to say at the outset, today's episode is going to provide an overview of data protection and Jon and Helen will highlight some of those key considerations that all employers need to be aware of. We will be exploring in more detail some of the more complex HR challenges in some deep dive episodes later this year. For example, AI and data protection in the recruitment process and also the quite complicated area of data subject access requests.

Ellie: First of all, Jon, can I ask you why is data protection such a hot topic at the moment for businesses?

Jon: Thanks, Ellie. Well, there's always been a clear link between data protection and in the context of employment. mean, aside from customer data, employee data is often the most significant repository of personal data that employers have. And it's often the most sensitive data repository as well, given that it will often include data around health and ethnicity and so on. But certainly there has been an increased focus in compliance in recent years. We saw it initially back in 2018 with the advent of GDPR, massively increased the scope of obligations on organisations and a huge increase, of course, in the potential consequences with the fines regime that we can talk about later. We've also seen a big increase in recent years on the volume of data being processed, the global nature of supply chains the innovations in how employee data can be processed for productivity and efficiency and so on. And of course, we're now in the last year or two in the foothills of an AI revolution, which is going to generate a huge focus on investment in AI to use employee data in ways that in some cases will have greater risk profiles. We're certainly seeing more requests for risk assessments on AI projects within the sort of HR space that cut across both data protection and digital ethics and AI specific regulation. So for example, a recent example, we have a client in the hospitality sector that was looking at using AI or embedding AI within the CCTV that they use to monitor the hospitality areas, the customer areas. Ostensibly, the idea was that the AI would give them feedback, which would enable them to improve the efficiency of their staff within those areas.

But of course, you can see how that would lead to concerns around personal data processing. Is it going to be used for performance management and so on? And so that did require a risk assessment. And we're seeing more and more queries around this sort of deployment.

Ellie: So data advisory must be busier than ever. And Jon, you mentioned the sort of greater risks of getting it wrong. Can you give us some recent examples of enforcement in relation to employee data that have been particularly significant?

Jon: Well, in the UK we had quite a good example last year when the ICO, the Information Commissioner in the UK, enforced against Serco Leisure. So Serco operates a large number of leisure centres around the UK on behalf of local authorities and they had implemented facial recognition technology and in some cases fingerprint scanning technology at these centres to

use for their employees to both enter and exit the centres. So it was effectively used for clocking in, clocking out purposes. They would use it to monitor attendance times and therefore calculate employee pay off the back of this facial recognition. Now these technologies use biometric data, which under GDPR is special category data. And as we'll talk about a little bit later on, this kind of data can only be processed in very limited circumstances.

So Serco argued that it was necessary in order to perform their contracts with the employees effectively to pay them that they use this facial recognition access technology. And in order to justify the use of special category data, they said, well, we need this in order to comply with legislation, things like Working Time Regulations. But the ICO's view on this was that it was not necessary, which is the relevant threshold for this technology to be used. It was useful, but was it proportionate given that there were less intrusive options available. So effectively, Serco was ordered to stop using these systems, delete the data that it had collected. And so they weren't fined, but they were, you know, they were required to make significant operational changes across all of these centres. And in another example, I can give you from around about the same time, there was a big fine. This is the French data regulator, fined Amazon a whopping 32 million euros. And in this, in this case, it involved a logistics warehouse operated by Amazon in France, which issued staff with handheld scanners. And the idea for these scanners was to document every single action. So you take an item off a shelf, you pack an item in a box, you put an item in storage, everything was minutely scanned. There was a lot of granular data collected, even monitoring periods of inactivity, notably. And the French regulator considered that this monitoring was excessive. For example, it would put pressure on staff about the length of their breaks. They were holding the data for over a month. And the argument was, well, if you only need this data to manage your real-time logistics, why would you hold it for so long? you're going to be assessing employees' performance through this monitoring. So, you know, this is a big fine. This is big tech, of course, which does tend to receive bigger fines from data regulators. But certainly the monitoring of staff activity is a big focus for data regulators and I can only see that increasing with the era of hybrid working that we're now living in.

Ellie: Helen, before we look at the practicalities of data protection, can you just remind us of the key data protection principles that employers need to bear in mind throughout the employment life cycle?

Helen: Sure Ellie, yes, there are some key principles that employers must follow when they're handling their employees' personal data and that will help avoid some of the issues Jon's just been describing.

First of all, employers must have a lawful basis for their processing of employee personal data. So all the data processing that employers carry out, be it processing financial data for payroll, reviewing employee performance in review meetings, or indeed obtaining and recording sensitive information such as health data for sickness absences, must have a lawful basis as set out in data protection law.

Now there's a limited list of those lawful bases and the processing must fit into one of those scenarios. And these include processing necessary for the employer's or a third party's legitimate interests for performance of the employment contract or to comply with a legal obligation. And as you might expect, sensitive data, which includes things like health and disability data, racial or ethnic origin, trade union membership, these are treated with even more carefully by the law and there are more limited circumstances in which they can be processed. Similarly, for criminal conviction and offence data, the rule is basically that you can't process it unless it satisfies one of the limited conditions set out in the Data Protection Act. And these allow, for example, for background checking of employees in certain circumstances. It's worth mentioning actually that you can process personal data if you have the consent of the individual. But consent is problematic in the employer employee context due to the perceived imbalance in power in the relationship, such that a consent is generally considered not to be a true consent because it can't be freely given by the employee to the employer. Therefore, generally it should be avoided as a lawful basis by employers unless there are no other lawful bases available.

Even then, you just need to carefully work through and consider whether consent can be freely given by the employee in that particular context. Next one is fairness and transparency. It must be clear to your employees how and why you process their personal data. This information is typically provided in the form of an employee privacy notice. But beyond making sure you've put in place an employee privacy notice that ticks all the boxes and complies with the law, it's really important to just follow the general rule of thumb that the processing should be within your employees' expectations. It's important just to ask yourself would they expect you to process their data in this way? And if they wouldn't, then it's more likely that it's not lawful. It's very important to keep data secure generally. And remember, you should consider the increased security that might be required for HR data especially sensitive data. That would be things like limiting access to sensitive information to a restricted list of employees, applying audit control so you can check and monitor access to the data, and applying things like password protection. Security is of course not a once and done obligation. It should be reviewed and updated as needed on a regular basis to ensure it remains fit for purpose. And you should keep a record of any security breaches and assess and implement any remediation or mitigation measures required. Data minimisation and deletion. You should collect the minimum necessary for your purposes, the minimum amount of data. It's important not to collect data just because it would be nice to have or interesting to know. It should just be limited to what you need to know about your employees to manage the relationship. Data should be deleted as soon as it's no longer required in line with your

documented retention policies. Of course, beyond complying with this obligation with this principle of data protection law, there are great benefits in minimising and deleting data promptly. It reduces the risks associated with security breaches. So the less the data that's impacted by a breach, the more you reduce the adverse impact and the risks to employees and to the business.

And of course it reduces, you know, the less data you hold, the less data you have to sift when you're responding to subject access requests. And it avoids the need to kind of process lots of irrelevant or excessive data. You should make sure data is accurate and kept accurate. And how do you do that? Well, it's about careful recording of data that you receive and ensuring you have good data management processes, which I think Jon will discuss in a little bit more detail later and you should implement required changes to data promptly. Of course it's not all on you as the employer, it's appropriate to in many cases to put an onus on employees to keep their own data up to date and that can be particularly in circumstances where you know in companies where employees have access to their own data via their HR, your HR portal.

And then remember purpose limitation. You should only use the data that you've received for the stated purpose. And by that, I mean the purpose that you've set out and explained to employees in your privacy notice or elsewhere. You shouldn't use it for any unconnected purpose that you haven't told your employees about. Just remember what we're talking about earlier. Would your employees expect this use of their data? If they wouldn't, you need to have a think about that work out whether it's lawful and whether you should be doing what you want to do with it. Finally, employers are accountable for their actions in relation to personal data. If there's a complaint or issue, the burden will lie with the employer to demonstrate that it's acted in accordance with the law. The burden is not on your employees to demonstrate that you've fallen short.

Therefore, it's really important to keep full and accurate records of your processing. For example, detailed data mapping, knowing how your data is processed, where it goes, keeping records of your data protection impact assessments, and also actually keeping clear records of how you've sifted and how you've retrieved and identified relevant data in response to a subject access request. And this is all really helpful so that you're ready and able to evidence compliance if you ever receive a request from a regulator or a complaint from an individual.

Ellie: Thanks Helen, some really useful practical ways of handling and making sure data is protected correctly. So in the employment context, Jon, as you've both mentioned, we're often talking about fairly sensitive personal data. So what does that mean legally?

Jon: Well, to start with any information about an individual will be personal data that's regulated by GDPR as a starting point. So name, address, email, CV, performance appraisals, pay slips. So you do need to comply with data protection law, of course, in relation to all of our personal data. But there is a limited and very specific list of data types that Helen alluded to a moment ago, known as special category data under the old regime.

Pre-2018, was called Sensitive Data, but it's called Special Category Data now. And the law is much more restrictive about when and how you can use Special Category Data. The list is mainly the following. So it's sort of health or disability data, biometric data, genetic data, data relating to race or ethnicity, religious beliefs, sex life or sexual orientation, and trade union membership.

And the reason for this list and why the regulators have historically sort of focused on this particular list is it's the sort of data that can lead to discrimination or adverse treatment of individuals, which is why even though we would all consider financial data such as salary information or credit card details to be sensitive, quite rightly, but it doesn't qualify as special category data for that reason. And there are similar rules, by the way, that I'm about to describe and in relation to criminal offence data so that it isn't strictly special category data, but it's subject to a very similar regime. And with this kind of data, there's very limited number of purposes that you can collect it and use it for. So with non special category data, as Helen alluded to, you have to find a lawful basis for using it, whether it's consent or legitimate interests or one of the other available lawful bases.

The special category data, not only do you have to do that, but you also have to work your way through a list of conditions and see if you can squeeze within one of those conditions if you want to process that special category data. So there's almost like a two stage lawful basis process almost to try and get to whether you're not whether or not it's justifiable to process. Helen mentioned explicit consent is an option for special category data, but as she explained in the context of employment, it's very, very unlikely to be valid you very quickly move on from explicit consent and look for other things such as equal opportunities, detecting unlawful acts, those sorts of things. And you'll find that list of there is a sort of a list of conditions within the legislation. If you can't satisfy one of those conditions, then you shouldn't be processing this kind of data. And even if you can satisfy the condition, you do need to take greater care over the use of special category data. And you'll often need to produce additional documents to ensure you're accountable such as impact assessments or what's called appropriate policy documents. So all in all, use of this kind of special category data does raise the bar for compliance.

Ellie: Now, of course, different data protection challenges will arise at different stages of the employment lifecycle, starting with, of course, recruitment. And as I mentioned, we will be doing a deeper dive into the interplay between AI in employment, including recruitment, and data protection in an upcoming episode. But for now, Helen, can you just highlight some of the key points for employers to bear in mind when they're processing data for recruitment purposes?

Helen: Yes, I mean to start with, employers should give careful consideration to how they phrase questions on their recruitment forms and the information that they request from candidates. It's really important to check that they are phrased appropriately and that they're not requesting information that you don't need for your recruitment purposes. Secondly, I think another issue that comes up a lot is in relation to automated decision making and AI, particularly in relation to sifting of applications from job candidates. It's important to consider the need for human intervention in the process and be very alive to the risk of unfairness in the system. So particularly unfairness that may arise relating to sifting or identifying people relating to protected characteristics.

And employers should be ready to sort of interrogate the tool and adapt it as needed to remove any bias that might sort of result from their use of these kind of systems. And you know, in extreme cases, be ready to abandon it if it produces unfair results. And just in relation to the whole issue of AI and recruitment, I know we're going to get into this in more detail in a future episode, but in the meantime, there's the ICO, the regulator has recently produced its audit outcome report on how to ensure AI recruitment tools protect job candidates' privacy rights and it's definitely worth a read if you're interested in this area. We have actually also covered it in the November 2024 edition of our data newsletter, Data Dispatch, which is available on our RPC website. Moving on, we also just wanted to highlight the importance of thinking about data retention. It's important not to keep data for longer than you should post- the recruitment process. Of course, you may wish to retain it for future or some information about candidates for future job opportunities, but it's important to make sure that you've explained that to candidates. They understand if and how their data will be retained and to make sure you have a lawful basis to do so. As we mentioned before, important to delete data when it's no longer required and in line with your documented retention schedule. Although some likely limited records may need to be kept for longer than other details, just to have a record of recruitment decisions. And again, transparency, do candidates understand what data you are collecting on them and how it will be used. And just to flag again the importance of ensuring you provide a suitable job candidate or recruitment privacy notice to your job candidates. And then on management of subject access requests, we are seeing an increasing number of rejected candidates bringing subject access requests to dig into why they were rejected from a job application especially if they think the decision may be related to a protected characteristic or disability. And I think it's important to remember that comments and decisions relating to that decision can be readily challenged when they're obtained by way of a subject access request. And employers should give quite a lot of thought to how employees are instructed, those who are involved in recruitment decisions are given clear guidance on how to record interview notes appropriately and communicate hiring decisions well. But we'll talk about subject access requests a bit later when we get into more detail on that in a future Work Couch podcast.

Ellie: And moving on now to post recruitment Jon, so once somebody is in employment, what kinds of data protection issues commonly crop up?

Jon: Well, of course, one of the risks that gets a lot of attention and I suppose press coverage is security breaches, so data loss. You still have a lot of that caused by human error, so the classic sort of laptop left on a train or sensitive spreadsheets being emailed to the wrong people. But of course, increasingly, we now have a lot of cyber style data breaches, although even those are often due ultimately to some human failure. So for example, you often get phishing or other social engineering attacks where people inadvertently will hand over their credentials. But beyond the security breach, which I guess is the company's every company's nightmare scenario, we're often focusing on advising around on risk assessing implementation of new technologies that are going to be deployed in the workplace mainly for the companies that want to use that technology, but we also advise the software providers themselves. And because even if the providers themselves are just processes of the personal data that will be collected in their systems, and therefore a lot of the compliance requirements sit with the customers, they do have to be on the front foot with things like privacy by design and other aspects if they want to get traction in the market. So they need to risk assess their tools, their software in anticipation of questions from their corporate customers. So you'll see we see it on both sides and we'll often be producing data protection impact assessments or indeed transfer impact assessments where personal data is going to be processed outside the UK or the EU.

I touched earlier on with a couple of case examples on things like biometrics and employee monitoring and surveillance and they are definitely issues that we're increasingly seeing come up in terms of regulatory attention and of course the increasing use of AI. think we're getting to a period now over the next couple of years where a lot of these tools will be implemented in enterprise HR tools and they will be increasingly hot topics for compliance and enforcement. We're also seeing employees themselves increasingly want to deploy their own personal AI devices in a work context. So for example, note taking tablets or small devices that record meetings and then transcribe the content of those meetings, produce summaries and action points all through AI. And this is great technology from productivity perspective. It can save people a lot of time, but of course it does generate issues that you inevitably get with sort of shadow IT around confidentiality, data protection, data security, and so on. So we're certainly seeing that encroaching more with the development of what we might call consumer AI. And then finally, and as Helen touched on a moment ago, know, the big compliance headache in the context of employment is the rise in weaponised DSARS, where you get disgruntled employees or ex-employees or job candidates who will bring DSARS and they will be quite painful quite often if they're broadly scoped and a company holds a lot of data on employee, can, you know, they can be very resource intensive. We provide an outsourced DSAR service to many of our clients and we deploy a lot of technology to smooth the process and make it more manageable, but it's still a challenge for a lot of our clients to manage them. And we see that increasing in frequency. I think it's partly due to an increase in awareness and certainly it's become a sort of default arsenal, I suppose, in any employment claim. Prior to any significant action being taken, you'll see a DSAR being thrown in at an early stage.

Ellie: Thanks, Jon and on that point, we'll continue the conversation on data subject access requests in part 2 next time, and you'll also be giving your top tips for avoiding the worst consequences of breaching data protection obligations. We'll also take a look at what's on the horizon for data protection law this year. For now, though, thank you both so much for providing that really helpful overview of some of the key risk areas that employers really need to be alive to – and we'll look forward to you coming back on The Work Couch very soon for part 2!

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. 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.