XpertHR Weekly Podcast

Original XpertHR Podcast Sarah Thompson: 2 December 2016

Laura Merrylees: Hello and welcome to this week's XpertHR podcast, with me, Laura Merrylees. In this week's feature length edition podcast, we're discussing the EU General Data Protection Regulation, or the GDPR as it's commonly known, which comes into effect on 25th May 2018.

Now, 2018 may feel far away at the moment, but there's a lot of work to be done between now and then to make sure your organisation will be GDPR compliant and as we'll hear today, many of the new requirements fall squarely in the realm of HR.

The GDPR's new enforcement system is also no laughing matter, with potential fines of up to €20 million or 4% of an organisation's global annual turnover, whichever is the higher. So joining me on the phone today to talk thought what the GDPR means for HR is employment lawyer and Certified Information Privacy Professional Sarah Thompson, from McGuireWoods, London. Sarah, before we get into the detail of the GDPR, can you just tell us a bit about why it's being implemented? Doesn't the EU already have data protection legislation? [01:10]

Sarah Thompson: Yes, but currently data protection law across the EU is based on a number of national laws that implement the EU Data Protection Directive in different ways. So one of the purposes of the GDPR is to harmonise data protection law across the EU. It's done so in the form of a regulation that is directly applicable to all EU Member States, without the need for local implementation. Another reason for the creation of GDPR is that because the current directive is over 20 years old, it's not kept pace with technological developments. So by way of illustration, the Directive was agreed years before Facebook, Twitter or even Google existed. The GDPR overhauls the current law in light of the ever changing technology landscape. [01:49]

Laura Merrylees: Okay, now before we go any further, let's just address the issue of Brexit. The GDPR is EU law. Will Brexit affect its implementation in the UK?

Sarah Thompson: Well the GDPR will come into force before the UK leaves the EU and as I mentioned it will be directly applicable to all EU Member States, including the UK, without the need for any additional legislation. So employers will need to be compliant come May 2018 or risk the GDPR's significant fines.

Laura Merrylees: And what about after Brexit?

Sarah Thompson: Well after Brexit we don't know if the Government will make changes to the UK Data Protection Law and much will depend on the future relationship between the UK and EU. For example, if we also leave the EEA, we will need to demonstrate adequacy in order to continue transferring personal data with the EU. In practise, this will amount to demonstrating equivalency with the GDPR and so it is likely that the UK will need to put in similar legislation.

Laura Merrylees: All this is to say that regardless of Brexit, employers should implement GDPR compliance plans to ensure that they have all their ducks in a row by the May 2018 deadline?

Sarah Thompson: Yes. That's certainly our recommendation. The Information Commissioner's Office, the UK's data protection regulator, will also be publishing guidance over the coming months which will help employers understand how it will be interpreting the GDPR in the UK. [03:03]

Laura Merrylees: Well I'm glad the Brexit issue's settled, at least regarding the GDPR. Now the GDPR is a large piece of legislation. Can you give us an overview of how it will work and the main areas of change that employers should be aware of?

Sarah Thompson: The GDPR will in any ways be similar to the Data Protection Directive, which is implemented in the UK by the Data Protection Act 1998. The GDPR regulates personal data, which is any information relating to an identified or identifiable individual. This is generally the same type of data regulation as the current Data Protection Act. The GDPR requires employers to process personal data in compliance with data protection principles, which are also similar to those under the Data Protection Act and will be familiar to employers.

Laura Merrylees: And I understand that there is a new accountability principle? Is that significant?

Sarah Thompson: Yes. The accountability principle should generate a shift from paper-based compliance to actual and demonstrated compliance in practise. Employers will need to show compliance with GDPR requirements through, for example, policies, processes, employee training and extensive record-keeping of all data-processing activities. [04.06]

Laura Merrylees: That's interesting. So there's going to need to be a change of practise to comply with this principle. Are there other changes that will be significant for employers?

Sarah Thompson: Yes, there are quite a few. The GDPR changes the way employers can justify processing personal data, specifically in relation to consent. It requires organisations to provide more information to data subjects on why and how their data is being collected and processed, and also strengthens data subjects' rights.

The GDPR also creates additional consideration for data transfers outside the EEA, new requirements for data processors and notification requirements for data breaches. All of the regulatory changes are supported by an enforcement system, with significant maximum fines of up to €20 million or 4% of global annual turnover, whichever is higher. [04:48]

Laura Merrylees: Okay, so it's those fines that we mentioned earlier. They seem to be a good reason to take the GDPR seriously.

Sarah Thompson: Yes, absolutely. The fines have caught a lot of public attention, because they are considerably higher than the maximum fine that can currently be imposed, which in the UK is £500,000. The level of fine in the GDPR will very much depend on the type of breach and any mitigating factors in the circumstances. But they are certainly meant to penalise any organisation's blatant disregard for data protection rights. [05:17]

Laura Merrylees: And the GDPR applies to all organisations, regardless of their size, doesn't it?

Sarah Thompson: Yes, that's right. Organisations of all sizes fall under the GDPR and, while it seems unlikely that small organisations would breach the regulations in a way that would make it subject to the maximum fines, the GDPR requirements and its enforcement system generally apply to all organisations.

There is an exception to this statement, in that organisations with less than 250 employees are exempt from some of the record-keeping requirements for their data-processing activities, unless those data-processing activities are particularly high risk. [05:50]

Laura Merrylees: Alright, now that we know what's at stake, why don't we get right into the numerous changes you set out. Can you tell us about the changes to consent under the GDPR? That's a big one for employers, isn't it?

Sarah Thompson: Yes. That's right. Under the GDPR, all processing of personal data has to be justified by one of several legal grounds. Currently, many employers rely on employee consent, but this approach has been increasingly criticised. The reason for that is that for consent to be valid, it must be freely given and there is doubt as to whether consent is really freely given in a subordinate employer/employee relationship.

Laura Merrylees: So how does consent work under the GDPR?

Sarah Thompson: There will be strict requirements for user consent under the GDPR. It must be given by a clear, affirmative action and it has to be freely given, specific, informed and unambiguous. Also, where an employer processes sensitive personal data, for example health data or information about trade union membership, consent must also be explicitly given in relation to that sensitive data.

When consent is given in a written document that contains other matters, it also has to be clearly distinguishable from the other matters in order to be valid. [06:54]

Laura Merrylees: Okay, so, for example a generic consent that you might commonly find in an employment contract won't now be valid, presumably, under the GDPR?

Sarah Thompson: Yes, that's right. It does seem unlikely, because the employment contract contains matters other than data protection provisions.

It's also worth noting that individuals will have the right to withdraw consent at any time and to ask their data to be deleted for which consent has been withdrawn. So to the extent that any employment related data-processing relies on consent, if it is withdrawn, the data-processing would have to stop.

Laura Merrylees: Okay. So how then will employers be able to process employee personal data under the GDPR?

SARAH THOMPSON: Well there are several potential legal bases that could be used to justify processing personal data instead of relying on consent. What this means in practice is that employers will need to reassess their legal ground for processing personal data. Where consent is relied on, they should check whether it meets all the GDPR requirements and remember that free consent means that it may be revoked at any time. In many instances, employers will need to rely on one of the other legal grounds to continue to process the personal data. [07:54]

Laura Merrylees: Okay, so other than consent, what are the other legal grounds that employers will have to process data?

Sarah Thompson: Well, employers can rely on either contractual necessity, for example in order to process salary payments. They could also rely on the fact that they need to fulfil a legal obligation. So, for example, processing personal data in relation to tax and national insurance contributions. Or, on the ground that it's necessary for the legitimate interests of the employer. For example, in the context of employee monitoring.

Laura Merrylees: So will relying on the other legal grounds make it more difficult to process data going forward?

Sarah Thompson: Yes. Each of the legal grounds has restrictions that can only be used in certain instances. We've already discussed the restrictions around using consent. Another example is employees have the right to object to processing that is justified as being necessary for the legitimate interests of the employer.

So since the legal grounds for processing data under the GDPR are narrow, it may be that the employer will have to stop processing personal data, or at least limit the range of data processed if it doesn't fit under one of the grounds for processing. [08:51]

Laura Merrylees: Okay, then, so to summarise, the changes to consent under the GDPR mean that employers should review the personal data they process to make sure that processing is legally justified under the new system. They may be able to justify processing on several grounds, such as contractual necessity or the legitimate interests of the employer, is that right?

Sarah Thompson: Yes, that's right.

Laura Merrylees: If an employer wants to use consent as a justification, it will need to make sure that the consent meets the new stricter requirement under the GDPR.

Sarah Thompson: Yes. I mean that's not to say that consent cannot still be obtained and used alongside one of the other justifications, but it should not be the

only basis to justify the processing. If an employer is not able to find a valid reason for processing certain data under the GDPR, whilst this may be unlikely in the employment context, the employer may have to stop processing it, or at least limit the type of data it is processing. [09:39]

Laura Merrylees: Right, so that's the legal basis for processing personal data. You mentioned earlier that under the GDPR employers will also have to provide additional information to employees and job applicants about data processing. Can you just tell us more about this?

Sarah Thompson: Yes. Under the existing Directive, employers are required to provide employees and job applicants with a privacy notice setting out certain information. This information must be concise, transparent, easily accessible and given in plain language.

Under the GDPR, employers will needs to provide more detailed information to employees and job applicants in order to comply with the new data protection principle of transparency.

Laura Merrylees: So currently my understanding is that a privacy notice has to state the identity of the controller, which for our purposes is the employer, the purpose for which data is being processed and any extra information that needs to be given in the circumstances to be able to process the information fairly.

Sarah Thompson: That's right. The GDPR builds on this and also requires information about, for example, the time period for storing the data, the legal basis for processing the data, countries or organisations that the data may be transferred to and the level of protection afforded during that transfer, and also the data subjects' rights. [10:46]

Laura Merrylees: So when and how should employers be providing this information to employees and job seekers?

Sarah Thompson: Well for current employees the employer will need to implement a new data privacy notice or update their existing one. They would alert employees to the changes as they would when updating any other staff policy.

For job seekers, the new privacy notice will need to be given before individuals apply for the roles and provide their personal data. So, for example, if applicants complete an online application form, the privacy notice should be provided on the website and the applicants asked to click on a consent button before they can move on and fill out the application form.

And for new employees the privacy notice can be given alongside the other on-boarding policies. So, for example, with a staff handbook. [11:26]

Laura Merrylees: And apart from the right to be provided information on how their personal data is being processed, I understand that there is a suite of data subject rights, with the most common one employers have to deal with being subject access requests. Can you just tell us how this currently works?

Sarah Thompson: Sure. So data subjects, including employees, have the right to get a copy of the information that is held about them. This is knows as a subject access request. The individual can ask an organisation, so, for example, their employer, for copies of the records with their personal data. Organisations can currently charge a fee of up to £10 and must respond to a data subject access request within 40 days of receiving it.

Laura Merrylees: So what will be changing under the GDPR then?

Sarah Thompson: Well, instead of being able to charge £10 and having 40 days to respond to requests, employers will not be able to charge a fee and will have to respond within one month, although an extension will be possible for complex requests.

Laura Merrylees: So it sounds like this process, which is already quite burdensome for employers, will be getting more onerous, in fact?

Sarah Thompson: Yes, exactly. Subject access requests by employees are particularly difficult to respond to, because much employee personal data is unstructured and housed in different areas of an organisation. Under the GDPR, it's likely that such requests will become more frequent and more difficult to administer. [12:33]

Laura Merrylees: Alight. So just to recap so far, we've covered how organisations will need to justify processing personal data under the GDPR, what kind of information about data-processing they need to give their employees and the changes to Data Subject Access rights.

Now, once an employer has collected employee data, it's quite common for that data to be transferred out of the EEA. So, for example, if an organisation's HR database is located in the US. What are the requirements for protecting personal data in these cases and are they going to significantly change under the GDPR?

Sarah Thompson: Well overall the scheme on data transfers is materially the same under the GDPR as it is under the current Data Protection Act. That is personal data transfers outside the EEA are only allowed if certain protective measures are put in place. So this would apply, as you said, where an organisation's employee database is located outside the EEA.

Under the GDPR, data transfer requirements will apply for the first time to transfers to data processors. So, for example, agents and suppliers who process data on behalf of an organisation. This means that where employers transfer HR data to say benefit or payroll providers outside the EEA, both the employer and the processor will have to comply with the GDPR requirements. [13:44]

Laura Merrylees: That's interesting and what about the protective measures themselves?

Sarah Thompson: The existing methods of transferring personal data outside the EEA will continue to be recognised, but there will be some improvements to compliance requirements. So, for example, the GDPR removes the need to notify standard contractual clauses to data authorities and also encourages the development of codes of practice and

certification schemes for transfers. The EU Commission will also have the power to deem that certain territories, sectors or international organisations offer an adequate level of protection for data transfers, which will remove the need for special protection for such transfers.

Laura Merrylees: So there's quite a lot to that. What does it in fact mean for employers?

Sarah Thompson: Well employers will need to consider their existing and proposed future transfer arrangements, including to data processors, and assess whether they will be sufficiently protected. They will also have to keep records of transfer solutions adopted, although the exemption for employers with less than 250 employees that we discussed earlier applies here.

Laura Merrylees: Okay. So employers will have to conduct an audit and they'll have to put into place policies and record-keeping requirements, just as they will have to do for their own internal data flows, presumably?

Sarah Thompson: Yes. Exactly. [14:48]

Laura Merrylees: Picking up on what you said about data processors being covered under the GDPR for the first time, aside from the international transfer requirement, are there other ways that this will affect employers?

Sarah Thompson: Yes. The GPDR, like the Data Protection Act, requires a written contract to be put in place for data processors. However, under the GDPR, more prescribed terms must be included in data-processing agreements than are currently required. In addition, because the processors will be directly liable, it is very likely that they will want to renegotiate their contracts to account for any increased cost or liability for GDPR compliance.

In practice, this means that employers will need to review their existing contracts with third party providers and if they do not comply with the new contractual requirements, new contacts will need to be negotiated and put in place. [15:30]

Laura Merrylees: Okay. So we've mostly looked at what you might consider preventative or protective requirements under the GDPR and those that ensure that data processing takes place in accordance with data protection principles at the collection and processing stage.

But the GDPR also requires organisations to put into place what you might consider, I suppose, responsive systems after there has been a data breach. Can you just tell us a little bit about those, Sarah?

Sarah Thompson: Sure. So a data breach is basically a breach of security that results in unauthorised destruction, loss or disclosure of personal data. They are quite common. For employers they might involve employees committing a data breach, for example, an employee could send an email to the wrong recipient or accidentally forget his laptop somewhere. A data breach could also involve disclosure of employee personal data. For example, if a personnel file is inappropriately accessed.

Laura Merrylees: And what will employers have to do then when a data breach occurs?

Sarah Thompson: Well, under the GDPR, organisations will have to notify the data protection authority within 72 hours of suffering a data breach. The notification must describe, amongst other matters, the nature of the breach, the likely consequences of the breach and the measures proposed or taken by the company. Organisations also have to notify data subjects without undue delay where the breach is likely to result in a high risk to the rights and freedoms of the individual. If a breach involved disclosure of employee personal data, this means that employees might have to be notified. [16:51]

Laura Merrylees: Will organisations have to issue notifications in all instances of data breaches?

Sarah Thompson: Well notifications have to be made where a breach is likely to result in a risk to the rights and freedoms of individuals. This has to be assessed on a case by case basis. The ICO has provided some examples. So, for instance, where organisations have a lot of customer details where the breach leaves the individuals open to identity theft, then notification will be required.

However, the loss or inappropriate alteration of a staff telephone list would not normally meet this threshold. There are also a few exemptions to the notification requirements. For example, if the data was encrypted.

Laura Merrylees: But how should employers be preparing for this particular requirement?

Sarah Thompson: Well we recommend that employers develop a data breach response programme, so that they are able to respond to breaches in the short timeframe provided. This will involve, for example, training the employees to recognise and address data breaches, allocating responsibility to investigate the breach and to make the report and putting appropriate policies and procedures in place. Employers will also have to keep a record of all data breaches and the actions they took in response, including breaches where no notification took place. [17:56]

Laura Merrylees: Okay. Thanks. Sarah, we've covered a lot of ground and I have to say the GDPR is an extensive piece of legislation and implementing it can seem a bit of a daunting task. Can you just set out a couple of next steps for employers to get started with their compliance plans?

Sarah Thompson: Sure. Well the first step for all employers is to understand what data they have, where it is and what they do with it. They can do this by carrying out a data audit. That is carefully assessing current HR data and related processing activities and identifying any gaps with the GDPR. For example, does their current employee consent with the new requirements? And if not, what justification will they have to process the data?

On the basis of this audit, employers can then consider what data collection and processing is truly necessary for the employment relationship. They should then put in place the required mechanisms to comply with the new obligations and update any policies and practices to reflect the changes. [18:47]

Laura Merrylees: And as we discussed today, there may need to be new or amended policies and procedures on, for example, providing information to employees and job applicants, for data-processing activities themselves, responding to data breaches, responding to data subject access requests, conducting international transfers and engaging of course with data processors. So overall there's a considerable number of issues for employers to put their minds to, isn't there?

Sarah Thompson: Yes, that's right. Other steps for employers to consider at this stage include considering who will take responsibility for compliance, and what position to take on liability and contract terms with third party processors. [19:22]

Laura Merrylees: Speaking of responsibilities, what will the role of HR be in complying with the GDPR?

Sarah Thompson: Well to meet the new obligations, cooperation and understanding of obligations across the business is critical and organisations are therefore likely going to need HR, legal, IT and compliance teams all to take a combined approach. The most important issues for HR to be involved with include auditing the grounds for processing employee data, assisting with data subject access requests, changing existing HR policies and practices and keeping accurate and up to date personnel files. [19:53]

Laura Merrylees: And are there timeframes that you'd recommend for employers to progress towards full compliance?

Sarah Thompson: Well as you said earlier, the GDPR will come into effect on 25th May 2018 and whilst that gives employers about eighteen months, it's critical to start preparing and commencing compliance efforts now. The ICO also advocates beginning work immediately and has issued helpful guidance setting out a framework of 12 steps to take now for organisations to follow.

Laura Merrylees: Well thanks very much, Sarah, for a really practical overview of the upcoming GDPR requirements. We can see that getting our ducks in a row for May 2018 will be no small task. So it's great to have your guidance in this area. You can look for more guidance on the GDPR in our trending topics section of the site.

Well that brings us to the end of this week's podcast, which you've been listening to with me, Laura Merrylees. We're back again next Friday, but until then it's goodbye from us.