XpertHR Podcast

Original XpertHR podcast: 9 June 2017

Jeya Thiruchelvam: Hello, and welcome to this week's XpertHR Podcast with me Jeya Thiruchelvam. This week we're going to do a quick primer on the EU General Data Protection Regulation, known as a GDPR. Joining me today is Employment Law Editor, Qian Mou. Qian, before we get into the GDPR itself, we are still getting lots of questions about whether organisations in the UK need to be preparing if we are going to exit the EU. [0:00:31:8]

Qian Mou: Well the answer to those questions Jeya is an unqualified yes. All UK organisations need to be preparing for the GDPR. So first off, we are still going to be part of the EU in May 2018 when the GDPR comes into force, and that means it will be directly effective in the UK as of that date.

Jeya Thiruchelvam: So directly effective is a term that has a very specific legal meaning that all of our listeners might not be au fait with. So what does that actually mean? [0:00:57:4]

Qian Mou: It means, the UK won't have to pass any additional legislation to bring the GDPR into force.

Jeya Thiruchelvam: And are there are any other reasons that the GDPR is going to be important? [0:01:05:09]

Qian Mou: Yes the Information Commissioner's Office, so that's the UK's data protection regulator, has said that the GDPR will have a significant impact on the future development of data protection law in the UK regardless of Brexit.

Jeya Thiruchelvam: Okay, so moving on, many of our listeners are already aware of the GDPR including the new fine regime up of to €20 million or 4% of group worldwide turnover, which is incredibly hefty. [0:01:29:02]

Qian Mou: Yes, the fines have received quite a bit of publicity.

Jeya Thiruchelvam: What we're hearing is that many of our listeners aren't sure how the GDPR will affect HR functions specifically. Because employers process a significant amount of personal data from job applicants and employees, the GDPR will have quite an impact on HR, and HR are likely to be heavily involved in compliance efforts presumably. So can you tell us about some of the roles HR will have during the GDPR compliance project? [0:01:55:9]

Qian Mou: Sure so one of the initial responsibilities for HR in GDPR compliance, will be to identify employee personal data, where it is stored and how

it's used. This is often known as a data audit or data map, and basically it starts with looking at personal data collected from job applicants and carries through the employment lifecycle. So it will cover data kept on HR systems and in personnel files, the data that managers keep on their employees and any other data an organisation collects on its workforce.

Jeya Thiruchelvam: You talked about a data map there, which is a term that has been banded around quite a lot. Is that a specific legal technical term and what does a data map look like? Does it sort of take a prescribed form? [0:02:39:02]

Qian Mou: So there isn't a prescribed format and it can take a variety of different forms as long as it fulfils the purpose of helping the organisation determine what personal data is collected, where it's stored and how it's processed.

Jeya Thiruchelvam: And what happens once the data map has been compiled? [0:02:56:02]

Qian Mou: Well, a couple of things. The GDPR requires a detailed record to be kept of personal data processing activities. So the data map can serve this purpose if it contains the necessary information. Secondly, and very importantly, the data map can also be used to identify gaps between the current practice and the requirements under the GDPR.

Jeya Thiruchelvam: Can you give us some examples of what those gaps might be? [0:03:19:05]

Qian Mou: Sure, so for example the GDPR will make significant changes to the use of consent to justify the collection and processing of personal data. We've had draught guidance from the ICO stating that consent will be very difficult to rely on in the employment context. What this means is that, using the data map, employers will have to look at all the different types of data they collect on their employees and in most instances, instead of relying on consent, determine a different legal justification for processing the data.

Jeya Thiruchelvam: Now there are several types of legal justifications that employers will likely rely on, such as that processing data is a legal requirement that's necessary to perform the employment contract or that it's necessary for legitimate interests of the employer. [00:04:00:1]

Qian Mou: That's right, employers will need to look at the types of employee data they process and the processing activities they use and determine which justification or justifications are relevant. If it's not possible to justify the processing activity with one of the available grounds, the organisation will have to stop processing.

Jeya Thiruchelvam: Okay, so once an employer has mapped its data and assigned one or more legal justifications for processing, will it have to communicate that information to its employees? [0:04:27:04]

Qian Mou: Yes, the GDPR has expanded requirements about the information that needs to be provided to data subjects, which in our case are employees. One of the new requirements is that the legal bases for

processing has to be notified to employees, along with other information about processing.

Jeya Thiruchelvam: And what about policies and processes. What will employers have to do to ensure that their HR practices comply with the GDPR? [0:04:50:5]

Qian Mou: Well the GDPR is introducing a new requirement of data protection by design and by default. This means that organisations have to take the appropriate technical and organisational measures to ensure that data protection is incorporated into all of their procedures involving personal data.

Jeya Thiruchelvam: So what does that actually mean for HR? What steps will they need to take? [0:05:11:01]

Qian Mou: Individuals in HR will likely be involved in reviewing their policies and processes to ensure that only data that is necessary is collected, that it's only processed to the extent necessary and that it's stored securely. Also that access to the data is limited and that it's destroyed once it's no longer needed.

Jeya Thiruchelvam: Okay, so we know that some of the main tasks HR will be involved in include the data audit, identifying any legal justifications aside from consent for processing employee data, updating privacy notices and reviewing policies and procedures to ensure that data protection by design and default are integrated. That's a lot to do, so do you a have some tips for getting started? [0:05:48:2]

Qian Mou: Yes, it can definitely be overwhelming. Because there is so much work involved and much of it will require co-ordination across other parts of an organisation – so for example co-ordinating with IT, with legal, compliance and with various business groups – it's really important to have board or executive level buy-in. GDPR compliance efforts will require significant resources in terms of employee and management time and also potentially for spending on technology and consulting services. So those amounts should be signed off and allocated to the project.

Jeya Thiruchelvam: I suppose the hefty fines and potential negative publicity associated with non-compliance should be more than enough reason to be able to get management buy-in? [0:06:30:4]

Qian Mou: Yes and another key change under the GDPR is that individuals will have greater ability to bring private claims against organisations for breach. So as you say plenty of compelling business reasons to make GDPR compliance a priority.

Jeya Thiruchelvam: And just briefly, once buy-in has been secured, how should organisations be moving ahead towards compliance? [0:06:51:02]

Qian Mou: The next steps are to put together a team with the skills and experience to implement a GDPR compliance programme, to conduct a risk assessment so that you can prioritise your compliance efforts, and to put together a compliance plan and timeline. So this would include the items that we talked about earlier, such as the data map.

Jeya Thiruchelvam: Great, so although we don't have time to go into all those steps today, we do offer some practical guidance in our How to guide on How to start preparing for the GDPR. [0:07:19:3]

Qian Mou: Yes, the guide has practical advice on the issues we covered today, as well as guidance for how to put together your compliance team, considerations for conducting a risk assessment and tips for putting together a compliance plan.

Jeya Thiruchelvam: Thanks Qian. We also have a number of FAQ's and an on-demand webinar that deals with various aspects of the GDPR. That brings us to the end of this week's XpertHR Podcast, which you have been listening to with me, Jeya Thiruchelvam. We're back next Friday, but until then it's goodbye from us.