www2.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2017/08/23/what-does-hr-need-to-know-about-gdpr.aspx

The answers to seven burning questions on the incoming legislation

The General Data Protection Regulation (GDPR) is due to come into force on 25 May 2018, giving HR departments less than a year to get their house in order as the way organisations collect and process data about employees and job candidates will be changing. Here's what HR needs to know now:

What happens to the idea of consent in the employment relationship?

At the moment, many employers gain consent to process employee data by including a clause in their employment contracts, but the GDPR will tighten the rules for gaining consent. "Consent now needs to be explicit, informed and given – and that means you can't just put it at the back of an employment contract," says Christine Young, employment partner at Herbert Smith Freehills.

HR departments should think about what reasons they could use to justify processing employee data, such as needing to do so to perform a contract or to comply with a legal obligation. Paula Barrett, global head of privacy and information law at Eversheds Sutherland, says HR should be using consent as a "last resort", particularly given growing rhetoric that employees are never truly free to give consent to their employer because there might be adverse consequences if they say no, as well as the fact that consent can be withdrawn at any time.

What will HR do if there's a data breach once the GDPR is in force?

Under the GDPR, organisations will need to disclose a data breach to the appropriate authorities within 72 hours. If the breach poses a high degree of risk to the rights of the individuals concerned, the business will need to inform the people affected as well.

"It's important organisations to have some kind of plan in place if there's a data breach," says Young. "Seventy-two hours is not a very long period of time to notify a regulator."

Do HR professionals need to be concerned about the 'right to be forgotten'?

The 'right to be forgotten' currently exists under EU law but the UK government has already said it will entrench the right into national legislation once the GDPR comes in. When most people think of the right, they think of Google removing links from search engine results, but Phil Allen – partner in the employment, pensions and immigration team at Weightmans – notes that the right to be forgotten could also affect information held on file about employees. This raises problems for HR departments trying to balance handling historic staff issues with the new obligations.

"To give you an example, if someone gets a warning for something, the Information Commissioner says that, once the warning's spent, you shouldn't retain those records," says Allen. "Most employers do retain the records because, when the same issue arises years later, they want to know that the issue happened before."

Barrett adds that this right might become relevant to HR if employees discover they have been holding on to more information than is necessary, or for longer than is necessary, to carry out an originally legitimate purpose. "Where I see the right to be forgotten kicking in more is where individuals say: 'Why have you still got my data? I want you to effectively stop processing that data,'" she says.

However, Young points out: "It's only limited to circumstances when a data subject can use that right. It's not a wholesale 'they've asked, therefore we must delete'."

What do I need to know about subject access requests (SARs)?

The rules around SARs are changing so, if one lands on the desk of the HR team post-GDPR, they'll need to respond more quickly. At present, companies have 40 days to respond, but this goes down to a month under the GDPR.

We use profiling in our recruitment. What do we need to know about the GDPR?

Using an element of automated profiling to filter through applicants – for example, hunting out CVs that mention certain skills and qualifications – is not uncommon, but organisations that do this will need to rethink their approach once the GDPR comes in.

"You need to notify people that you're doing this profiling and you may need to give them the opportunity to object to that and somehow have some human intervention," says Young.

How will Brexit affect the GDPR?

The GDPR stems from the EU but ministers this side of the Channel have already confirmed that the law will be enacted in the UK regardless of Brexit. Earlier this month, the Department for Digital, Culture, Media and Sport announced plans to introduce the rules under the data protection bill.

Young says: "For us to trade effectively with the EU, we'll need to make sure that we get an adequacy decision [a decision from the EU stating that the UK's data protection laws are adequate for trade purposes] so we'd need to make sure we had equivalence in protection."

How much do I need to worry about the fines?

With the maximum fine standing at 4 per cent of global annual turnover or €20m – whichever is greater – the potential penalties under the GDPR have garnered lots of attention. However, Elizabeth Denham, the UK information commissioner, has said these top-tier fines will be reserved for the most serious of breaches and will not be handed out for smaller infractions.

Related articles

Large fines under GDPR won't be the 'norm', says regulator

Experts urge employers to focus on their areas of risk rather than possible penalties

Fifth of Brits would ask employers to delete personal details under GDPR

Businesses urged to 'seriously think about overhauling' data processes – or risk falling foul of the regulations