UK Considers Changes to Data Protection Law

By Leah Shepherd
November 15, 2021

Employers in the U.K. should keep an eye out for possible changes to the rules governing data transfers and privacy.

On Sept. 10, the U.K. government introduced a consultation asking for organizations to submit their comments on the proposed changes to the country's data protection law. Businesses have until Nov. 19 to send their responses to the consultation.

The government will consider these responses and subsequently develop a legislative proposal. There is no set schedule for when that will occur.

With the new consultation, the U.K. aims to protect consumers and workers without blocking innovation and commerce. The government's goals include:

- Reinforcing the responsibility of businesses to keep personal information safe.
- Building on the use of data to tackle the COVID-19 pandemic.
- Securing the U.K.'s status as a global hub for the free and responsible flow of personal data.

Key Changes

Before Brexit, U.K. businesses were subject to the European Union's General Data Protection Regulation (GDPR). Post-Brexit, the U.K. has retained a national law that's similar to the EU's GDPR.

Here are four key changes proposed in the new consultation, according to Andreas White, an attorney with Kingsley Napley in London:

- Companies could charge nominal fees to individuals requesting a copy of their personal data processed by the company.
- The U.K.'s approach to cross-border data transfers would become more based on risk and outcomes, rather than on rigid comparisons of the text of legislation in the respective countries.
- Companies must have a simple and transparent process to handle complaints from individuals about transfers of their data. Individuals must try to resolve their complaints with the data controller before making a complaint to the Information Commissioner's Office.
- Companies would not have to fulfill data protection impact assessments, which are required under the EU's GDPR for data transfers that are likely to be high-risk to individuals. An example of this is when a person's medical information is processed.

"This is still only in the consultation phase, and it remains to be seen whether any of the proposals will be implemented," said Darren Isaacs, an attorney with Littler in London. "If the government wants to reform the data privacy regime, it needs to be careful that this is done in a way that doesn't make the EU question the U.K.'s standard of data privacy protection. If the EU considers that the U.K. doesn't provide an appropriate level of protection, it may decide that the U.K.'s laws are not up to EU standard, which will lead to an increase in compliance obligations when U.K. businesses deal with the EU."

Consequences for Noncompliance

Not complying with the U.K.'s data protection law can result in a fine of 17.5 million pounds (approximately 23.47 million USD) or 4 percent of the company's total worldwide annual revenue.

"Historically, instances of employer data breaches or noncompliance have not received significant penalties, except in very serious cases or where there are repeated breaches," Isaacs commented. "The U.K. data privacy regulator tends to take a reasonable and proportionate approach to policing the legislation."

Other possible penalties from the U.K. government include temporary or permanent bans on data processing, suspending data transfers to third countries, or ordering that data be erased or rectified, according to Joe Bryon-Edmond, an attorney with Herrington Carmichael in London.

Failing to keep personal data safe can lead to lawsuits from employees or former employees. "Increasingly we are seeing individuals, in particular ex-employees, use their data as a tool to bolster a grievance they have, often through data subject access requests," Bryon-Edmond said. "While they may be onerous, they need to be taken seriously. Too often, employers don't consider them a priority, which can lead to significant issues."

He urged employers to "get your house in order. It is never too late to start ensuring compliance, but sitting on it and not acting is what is most likely to cause issues. The Information Commissioner's Office will look more favorably on organizations that are trying to be compliant with the U.K. GDPR, compared to those that are burying their heads in the sand and ignoring it."

Deborah Margolis, an attorney with Littler in London, said a common mistake employers make is "not dealing with data privacy in a proactive way and only engaging with it when they face issues." Businesses should ensure that they properly document their compliance processes and that GDPR forms are part of their day-to-day operations from the outset, she noted.

It's too early to tell what proposed changes will ultimately become part of the law, Bryon-Edmond said. "Even if change is on the horizon, it is likely to take a sometime to implement, so that horizon is probably some way in the distance."

Leah Shepherd is a freelance writer in Columbia, Md.