GDPR and lawful basis: how to make sure you don't get caught out

By Dónall Breen* - 4 September 2019

Recently, the Greek Data Protection Authority (DPA) fined PWC €150,000 for incorrectly using consent as a lawful basis to process personal data. We look at what happened, and what can be done by UK employers to avoid a similar fate.

Lawful basis and GDPR

GDPR dictates how personal data can be processed by businesses, including about their employees. To process personal data, employers must have a lawful basis for doing so. A lawful basis is essentially the reason why the processing of personal data is necessary and GDPR prescribes six of these basis:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party.

It is up to organisations to decide which lawful basis is the most appropriate when processing personal data.

What were PWC doing?

PWC were processing data on the grounds of consent. This was found to be inappropriate in an employment relationship as employees must share personal data in order to continue with their employment and therefore consent is not freely given - a key concept of consent under GDPR. The Greek DPA found that personal data was actually being processed to allow effective operation of the company and that PWC should have been clear about this.

The basis of consent should only be applied in situations where individuals are freely giving their information and have ongoing control over how their data is used. Furthermore, it should also be easy for individuals to withdraw their consent. Typically, this will not be the case in an employment context as the personal data of employees e.g bank details, is often required to allow the business to run effectively. Therefore, the employer does not require the consent of the employee as there is a more appropriate legal basis to process their personal data. In addition to this, using consent as a lawful basis in an employment context would mean that employees would be able to withdraw their consent at any time, and if employees are able to do this then it is likely that this would have adverse consequences for the employee and possibly the business.

What does this mean for businesses in the UK?

As this incident was investigated by the Greek DPA, it does not necessarily mean the UK's Information Commissioner's Office (ICO) is planning on investigating similar breaches here. Nevertheless, the ICO can investigate any organisation under GDPR for any breach of data protection legislation. Therefore, it is advised that employers are transparent about why they are processing personal data and identify the correct legal basis for processing – especially in an employment context.

**Co-written by Amoy Daley. Amoy undertook an Internship at GQ|Littler in August 2019.*