SHEPHERD+WEDDERBURN

Countdown to GDPR
10 answers to common HR queries

With the deadline for GDPR compliance drawing close, we look at some common questions facing HR professionals in relation to employee data.

CAN WE STILL RELY ON CONSENT AS A BASIS FOR PROCESSING EMPLOYEES' PERSONAL DATA?

In short, no. Employers will no longer be able to rely on consent and will need to identify a different (legal) basis for processing.

Many employment contracts currently provide that employee consent is given to the processing of personal data (that is 'any information relating to an identified or identifiable living individual'). However, under GDPR consent must be freely given, and consent given as part of the recruitment process is not likely to be viewed as freely given and is therefore likely to be invalid. In any case, GDPR requires that an individual must be able to withdraw consent as easily as it was given, so a business could not logistically rely on consent as a stable basis for processing.

Some employers may have been considering requesting consent while also relying on an underlying basis for processing to cover them in the event that consent was found to be invalid or was withdrawn. However, the Information Commissioner's Office has criticised this approach as misleading employees who may think they have a choice in having their data processed when in reality the employer will process regardless of consent.

WHAT OTHER BASES CAN WE USE FOR PROCESSING PERSONAL DATA?

There are a number of legal bases that employers can rely on for lawful processing under GDPR and it is likely that employers will already have legitimate reasons for processing their employee data.

GDPR requires privacy by design and not as an afterthought. Employers should identify the legal basis for processing employees' personal data before they process that data. For example, processing may be 'necessary' for:

a. the performance of the employment contract, e.g. to pay salaries or make pension contributions;

b. the legitimate interests of the employer, e.g. for administrative purposes; or

c. to comply with a legal obligation, e.g. under the public sector equality duty.

There is no 'one-size fits all' for processing employee data. As such, employers should ideally carry out a data protection review to determine which bases it is relying on for different types of data processing.

WHAT ARE THE RULES FOR PROCESSING SENSITIVE PERSONAL DATA?

These special categories of data can only be processed with freely given consent, or if a specific legal basis applies.

GDPR updates the current list of 'sensitive personal data', re-brands this as 'special categories of personal data' and amends the definition slightly so that it now includes information revealing:

> *racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic and biometric data (for the purpose of uniquely identifying a person); health and sex life or sexual orientation.*

Employers will be particularly interested in the rules around processing health information for the purpose of managing sickness absence and making occupational health referrals.

As with personal data, relying on consent is problematic, as an employee would be entitled to withdraw that consent at any time. Consequently, employers need to identify whether another basis can be relied upon to permit processing. In the context of these special categories of data, there are a number of bases covering public interest, defence of legal claims, and necessity in order to comply with the employer's employment obligations. A helpful basis to rely upon when processing health information is where:

> *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.*

This ground will likely be relied upon by employers for the purpose of managing ill-health and to carry out occupational health assessments.

Before such data can be processed, the employer will still need to tell the employee what they are processing and why by issuing a Privacy Notice, as explained below.

DO WE NEED TO UPDATE OUR EMPLOYMENT CONTRACTS?

Yes, minor amendments will need to be made to employment contracts.

Template employment contracts should be updated going forward to reflect the new approach to data processing under GDPR and to remove reference to employee consent. For existing employees, it should be sufficient to issue an amendment letter, advising them of the changes. All employees should be made aware of how their data will be processed under GDPR, and issued with a Privacy Notice (see below).

DO WE NEED NEW POLICIES AND PROCEDURES?

A Privacy Notice will need to be prepared in relation to employee and job applicant data.

In addition to the changes to employment contracts noted above, employers will now also need to issue a Privacy Notice (also known as a fair processing notice) to all employees and job applicants. The Privacy Notice should contain details of:

- the legal data protection principles;
- the types of employee and candidate data being collected;
- the purposes / legal bases of processing;
- employee rights in respect of access to the data; and
- how data will be stored and how long data will be held.

Existing employees should be issued with a copy of the Privacy Notice by 25 May 2018. Thereafter, the Privacy Notice should form part of the standard job application and recruitment process. In addition, bespoke privacy notices may also need to be issued when new forms of data are processed or when the basis for processing changes.

When sending an employee to occupational health, you should consider whether you need to issue a bespoke privacy notice. If your standard Privacy Notice is sufficiently wide to cover this data processing, you will not need to issue a further notice. However, you may still wish to draw the employee's attention to the relevant part of the standard Privacy Notice. If your standard Privacy Notice is not sufficiently wide to cover such processing (or it is unclear), you should issue an additional bespoke privacy notice when data is actually being sent to occupational health.

In addition, employers should review their existing Data Protection Policy. This Policy may have wider application and may, for example, refer to the collection of customer or member data. However, in respect of employee data specifically, it should contain general information about the company's collection and use of personal data; the retention periods for different types of data; and the individuals that have access to personal data. It should also make reference to the Privacy Notice which will contain more comprehensive information on these points. The Policy should also address individual employees' accountability to comply with the policy when handling employee data, and the fact that a failure to do so may result in disciplinary action. In addition, the Policy should contain details of how any personal data breach would be handled, including one relating to employee data.

Steps should be taken to ensure that employees understand the new or updated policies. For example, employers may wish to prepare FAQs or run a training session for managers so they are prepared to answer any queries.

HOW LONG CAN WE KEEP DATA ABOUT STAFF?

One of the key principles of GDPR is that personal data should not be held for longer than is necessary.

Therefore, employers should consider whether to delete data periodically. Employers should carry out a review to establish the types of data held, where/how that data is stored, and to consider why it needs to be held for a given time period. For example, for employee records, there may be business reasons for retaining a full personnel file during employment. Protecting yourself from litigation risk may justify retaining this data for up to five or six years after termination of employment in Scotland or England respectively as this is the time limit for bringing a claim for breach of contract. The benefit of retaining information should be weighed against the potential drawbacks: the more data you hold the more onerous responding to a Subject Access Request will be for example. There may also be a storage cost of maintaining significant volumes of employee data and there is always the risk of a challenge that employers have held information for longer than necessary.

Some data has minimum retention periods: for example, for tax and HMRC purposes, payroll, salary and benefit data should be retained for seven years, and maternity/paternity pay records must be retained for three years from the end of the tax year in which the maternity or paternity pay period ends. Information about criminal record checks and spent convictions should also be deleted promptly in most cases.

Most HR departments will hold information about unsuccessful candidates such as CVs and interview records. However, normally it will not be necessary to retain this information for a lengthy period of time, and so a practice of deleting this information after a short period, for example between three to six months, would usually be appropriate.

Dealing with candidate data held in managers' email accounts may pose the biggest challenge for employers and it may be appropriate to require all such information to be held centrally.

For organisations operating document management systems (or similar) there may be a technical restriction on deleting information locally. Anyone operating such systems should review their operation to ensure that employees can easily comply with GDPR in relation to both the retention and deletion of personal data.

WHAT RIGHTS DO EMPLOYEES HAVE IN RESPECT OF THEIR DATA?

Subject Access Requests (SARs) will exist in substantially the same form, but there will be a few changes.

- The £10 fee will no longer apply. However, if the SAR is 'manifestly unfounded or excessive' a reasonable fee can be charged to cover administrative costs, or the employer could refuse the request altogether. There will no doubt be disputes regarding what 'manifestly excessive' means; however, the general aim is for employers and employees to agree on a reasonable scope of data requests and thereby minimise the instances where employers are required to engage a team of people for days reviewing many thousands of emails.

- The 40-day response period will be reduced to one month. If there are a number of requests, or if the request is complex, the period can be extended by a further two months. The individual must be informed of an extension within a month of making the SAR and there must be an explanation given as to why an extension is necessary.

- It will be possible to make a SAR by email, and if a request is made electronically then the response should also be electronic, unless otherwise requested by the individual.

- When responding, employers must also disclose information about the type of personal data held about the requester; the purposes of processing; and details of any third parties to whom the data may be disclosed.

Employees have the right, in respect of their data, to ask their employer to 'delete it, freeze it or correct it' in certain circumstances.

For example, an employee may exercise their right to erasure (delete it) if the employer has retained their data for too long or have no reason to retain it. However, an employer does not have to erase data that they need to retain under EU or UK law or where it is necessary to establish or defend legal claims. The right to object to or restrict processing (freeze it) can arise where the processing is unlawful, data is inaccurate or there is a conflict between the rights of the employee and the legitimate interest of the employer. The rectification right (correct it) can be triggered if inaccurate or incomplete data is held.

DO WE NEED TO UPDATE SUPPLIER CONTRACTS?

Probably.

Employers often outsource the processing of personal data to third parties or pass personal data to third parties for the purposes of receiving services (e.g. cloud hosting services sharing with group companies). Where an outsourcing contract involves the processing of personal data, mandatory processing provisions must be included in the agreement. The employer must satisfy certain requirements if data is transferred outside the EU, e.g. obtain the explicit consent of the data subject, or enter into the EU standard contractual clauses for the transfer of personal data outside of the EU. Businesses should review current contractual arrangements to ensure that these comply with GDPR.

9 WHAT ARE THE NEW RULES ABOUT REPORTING DATA BREACHES?

Under GDPR any personal data breach must be reported to the Information Commissioner within 72 hours of the company becoming aware of it.

Where individuals affected by the data breach are at high risk of their rights being infringed, for example through identify theft or fraud, then those individuals must also be informed of the data breach. A personal data breach is a 'breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.' For example, you could be responsible for an email containing an employee's address details being sent to the wrong recipient. 72 hours is a relatively short timeframe, so you should ensure there are response plans in place so that breaches are identified, reviewed and reported in time.

10 ARE THE RULES ABOUT EMPLOYEE DATA THE SAME ACROSS THE EU?

Unfortunately not.

While GDPR's aim was to harmonise data privacy across the EU and it has direct effect such that it automatically becomes law in each member state, employment provisions were one of the few areas where each country was given the power to legislate domestically and establish specific rules. This means that employers who operate across more than one EU country will need to ensure that they comply with the local laws on employee data privacy which, although based on the same principles, will not be exactly the same.

GDPR is introducing substantial fines of up to €20 million (or 4% of a company's global annual turnover, whichever is higher) for non-compliance so it is important to ensure you are prepared.

If you have any queries surrounding GDPR, please get in touch with the key contacts below or your usual Shepherd and Wedderburn contact.

Key contacts

Employment

Neil Maclean
Partner
T +44 (0)131 473 5181
E neil.maclean@shepwedd.com

Katie Russell
Partner
T +44 (0)131 473 5266
E katie.russell@shepwedd.com

Elouisa Crichton
Associate
T +44 (0)141 566 7249
E elouisa.crichton@shepwedd.com

Data Protection

Joanna Boag-Thomson
Partner
T +44 (0)141 566 8570
E joanna.bt@shepwedd.com

Paul Carlyle
Partner
T +44 (0)131 473 5782
E paul.carlyle@shepwedd.com