GDPR 2018

irwinmitchell

How GDPR Impacts on HR

Frequently asked questions

We recently delivered a series of workshops to HR advisors and business owners about the changes they need to make to comply with GDPR which is due to come into effect 25 May 2018.

This is a list of the most common questions we were asked.

1. **Do we need to undertake a data audit and, if so, what should this include?**
   We would suggest that if you have not already, you carry out a data audit in order to identify areas where action needs to be taken to ensure compliance with GDPR.

   There is no set way to carry out a data audit but, in general, you need understand the staff data that is held within your organisation; where that data comes from and where/how it is stored; what happens to it whilst it is within the organisation; and when and how it is deleted.

   You will need to consider these data processing activities in light of the requirements of the GDPR. Where you identify any areas of non-compliance, or where activities pose a risk to the business, you will need to formulate a plan to address them.

   The scope of the audit should include all staff personal data held in electronic format or contained within a structured manual filing system. It may be that you need to consider data stored or processed outside of the HR department, such as by finance, or a third party provider. Your audit may therefore have multiple stakeholders, and the timeframes necessary for carrying out this activity should not be underestimated.

2. **Our employment contacts contain clauses in which the employee consents to us processing their data. Can we continue to rely on these?**
   Probably not. Under GDPR consent needs to be specific, informed and freely given, which means that individuals should have a genuine and free choice as to whether or not to consent to the processing and should be able to refuse or withdraw consent without detriment.

   Current draft guidance from the Information Commissioners Office is that employers are unlikely to be able to rely upon consent as the lawful purpose for processing most employee personal data, because of the imbalance of power in the employer/employee relationship.

   There are, of course, other lawful purposes which most employer processing activities will fall under, but in accordance with the new accountability principles, you will need to be clear from the outset of the lawful purpose on which they are relying.

   It is very common within the UK for employers to have general "catch all" consent clauses within employee contracts or data protection policies. These will no longer be valid forms of consent, not least because they seek blanket consent for all employee data processing activities.

   Employers therefore need to review employment contracts and HR policies to identify where consent wording is used and consider whether this needs to be amended.

   If you no longer intend to rely upon consent as the lawful purpose for processing, you need to inform your staff and give them updated information about the lawful purpose that you do intend to rely upon.

3. **Does that mean that we cannot rely on consent at all?**
Not necessarily. If you want to rely on consent for any aspect of employee data processing, then in accordance with the guidance as currently drafted, you need to ensure that;
- Consent is a positive "opt in", separate from the other terms and conditions of employment. It should not be vague or encompass a wide range of issues. In addition the employee must be asked if they agree to their data being processed at least every 2 years.
- The form of consent is specific to the data in question and what you are using it for.
- If you are sharing the data, each 3rd party must be named and specific consent obtained from the employee in relation to each party.
- You advise the employee that they can withdraw their consent at any time and how they can do so.
- You keep specific records regarding consent to demonstrate compliance.

Please note: We are expecting the Information Commissioner to provide guidance on the issue of consent in the next few months which will, hopefully, clarify this issue.

4. **Do we need to make any changes to our HR policies and procedures?**
Yes. If you don't already have a data protection policy, now is the time to draft one. If you already have a policy you will probably need to make amendments to make sure that it sets out clearly the following information:
- What personal data is and why data protection is important.
- Information about your collection and use of personal data, the reason why it is collected and why it is processed.
- What the data rights of employees are and how you will ensure that these are upheld (see below).
- How data breaches are dealt with.
- The consequences, for your business and individuals, of non-compliance.

Other HR policies, such as IT, social media, flexible working and conduct policies may need to be reviewed and updated too.

Once updated policies and procedures are in place, make sure your staff understand them and keep compliance records to satisfy the accountability requirements of GDPR, and work towards preventing data breaches.

5. **How long can we keep information about our staff?**
This will depend on the nature of the information you are processing.

You will be required to review and update your data retention and deletion practices. You should have a written policy (as part of your Data Protection Policy, or a separate standalone policy) which sets out when and how specific categories of personal data are deleted.

Personal data will need to be retained for longer in some cases than in others. How long you retain different categories of personal data should be based on individual business needs.

However, keeping personal data for too long may cause the following problems:
- There is an increased risk that the information will go out of date, and that outdated information will be used in error.
- As time passes it becomes more difficult to ensure that information is accurate.
- Even though you may no longer need the personal data, you must still make sure it is held securely.
- You must also be willing and able to respond to subject access requests for any personal data you hold. This may be more difficult if you are holding more data than you need.

6. **Are there any new rules about data breaches?**
Yes. GDPR will introduce a duty on all organisations to report any data breach to the ICO within 72 hours, unless it is unlikely to result in a risk to the rights and freedoms of the individual affected.

Breaches will also have to be notified to the individuals affected where there is high risk to their rights and freedoms, e.g. identity theft, discrimination or fraud.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. For example; an employer could be responsible for a personal data breach if an employee's pay record is inappropriately accessed due to a lack of appropriate internal controls, or if payslips are sent to wrong person.

We recommend employers have an internal breach reporting procedure in place which should include;

- Guidance on what constitutes a data breach.
- Decision-making protocols about whether notification to the ICO or individual are necessary, who will be responsible for these .
- Recording systems for all breaches, including those where there was no obligation to notify the ICO, as the rationale behind that decision should be retained should you need to refer to it.

You may also need to consider amending other HR policies such as any the disciplinary procedure or any whistleblowing policy to give effect to the data reporting procedure.

7. Will our staff be able to make Subject Access Requests under the new regime?

Yes. GDPR enhances employee rights to access personal data held by their employers; entitles them to more detailed information regarding the way in which their data are processed; reduces the time limits for the employer's response and abolishes the current £10 fee for responding to a SAR.

This may encourage more people to make a SAR. Many already do so in an attempt to obtain information that they can use as "leverage" in other employment disputes.

It is worthwhile considering putting in place specific SAR protocols including template letters and carrying out an assessment of your organisation's ability to isolate data relating to a specific individual quickly.

As a minimum, we suggest that appropriate training and guidance is put in place to ensure that staff can recognise and respond to SARs quickly and efficiently and if they are considering refusing a request, they are aware of legal basis on which they may do so.

8. I've heard about the "right to be forgotten" – what does this mean for HR?

GDPR provides staff with a new right to require employers to delete personal data where:

- the data is no longer necessary for the purpose in relation to which it was collected;
- consent to processing has been withdrawn and the employer has relied on the employee's consent to process the personal data;
- the personal data was processed in breach of the GDPR;

protection policies and any data privacy notices that you issue to staff set out clear rules and guidelines about how an individual's 'right to be forgotten' will be complied with.

9. Do we need to train our staff about GDPR?

Yes. Properly trained staff can make all the difference, not only in demonstrating your organisations commitment to upholding the principles of data protection within the GDPR, but also in ensuring that staff data is properly and lawfully obtained, stored, processed and deleted and in helping to prevent any data breaches.

All staff should be trained in how to handle data. This training must be evidenced and monitored and updated..

We suggest specific training is provided for staff responsible for dealing with employee's data subject rights such as SARs or requests for data to be deleted, and for those responsible for data breach notifications.

10. Where can we obtain more help?

IM will be there to help and support you and your business every step of the way. In addition to employment matters, we have a team of experts in data protection compliance to help ensure that your HR team and wider business is fully prepared. We offer bespoke training; contract and policy reviews and specific guidance to meet your organisation's needs. Please do get in touch to discuss how we can help.

We also have a questionnaire which will help you think about how you handle people's personal information give you a good understanding of what you do well and where there is room for improvement. We can also discuss your answers with you /how well they demonstrate your compliance with data protection law.

Please ask us if you would like a copy.

Jennifer Walton
Associate Solicitor, Employment

T: +44 (0)114 274 4657
M: +44 (0)773 019 4346
E: jennifer.walton@irwinmitchell.com