hasslefree HR

Human Resources & Health and Safety

Data Protection Act 2018 (which includes the GDPR)

Frequently Asked Questions

We recently met with all our retained clients to discuss the new Data Protection Act 2018, which incorporates the General Data Protection Regulation. Throughout these meetings we were asked many questions, some of which were very similar, so we felt it would be a good idea to publish the frequently asked questions with our answers, in case any of our readers had similar queries. Our sources for this newsletter are the ICO and the CIPD.

What is personal data?

Personal data is defined as any information that relates to, or either directly or indirectly identifies, a living individual. For example, personal data could be a name, an identification number, a location, an on-line identifier, or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. If this information cannot identify an individual when used alone but can be used to identify an individual when combined with other information, then it falls under the description of personal data. Code names or pseudonymised data, such as an NHS patient number, can still be used to identify an individual and are therefore still classed as personal data.

Can a twitter handle be classed as personal data? By having twitter followers, are we storing the personal data or our followers, or are we not responsible for processing this personal data?

If an organisation is using a social media site like twitter simply to communicate with the public in a social way, there is no need to worry about the Data Protection Act 2018 because they are simply a customer of the site using the site as it was intended to be used. If an organisation is using a social media site for marketing purposes / to promote their services, the Data Protection Act 2018 may apply. For example, if they were sharing reviews via

social media, those reviews might be able to identify a person, and therefore the data protection principles would apply. Talking to someone via their twitter handle does not mean that an organisation is processing his or her personal data. Twitter is the party responsible for storing everyone's personal data, they seek consent and permission to do this, so organisations do not need to seek consent to interact with people as this would be an expected practice of the website. However, if an organisation was to download twitter handles to keep track of twitter followers, this would not be an expected action, and therefore this would need to be done in line with the Data Protection Act 2018 i.e. they would need a person's permission before they extracted the information from twitter. This is because a twitter handle may be classed as personal data if it can identify an individual. Twitter handles are not isolated, they are linked to a profile. That profile may have a photo of a person, it may contain their name, email address, the name of the city or town that they live in, and some even say when someone's birthday is. The exception to this would be if no personal information was shared on the profile and if there was no way you could discover the email address of the person.

At what stage does a job applicant need to be given a Privacy Notice? Is it when we receive their CV or when we invite them to attend an interview?

The ICO advises that you must provide privacy information at the time you collect or process a person's personal data, therefore every time a CV is received you would need to send a privacy notice to the data subject. However, the ICO also states that you do not need to provide individuals with a privacy notice if they already have the information or if providing the information would involve a disproportionate amount of effort. It would take a large amount of time and effort to send a privacy notice to every applicant during a recruitment drive, it would take even more time and effort when we consider the number of speculative CVs / applications employers receive each year. Therefore, the least time-consuming approach would be to have a copy of your "Job Applicant Privacy Notice" readily available either on your website or attached to the job advertisement, this way you would not need to provide the privacy information to each applicant because they would already have access to it.

If an employee signs their contract of employment, are they giving me consent to process their personal data?

No, an employee signing their contract of employment does not mean they are consenting to the way their personal data is processed. This is one of the changes introduced by the Data Protection Act 2018 (and GDPR). Previously employers could assume that the lack of an objection meant consent was granted, now consent must be both explicitly and freely given. There can be no assumptions, and for consent to be freely given, it cannot be addressed in a document an employee is expected to sign, such as a contract of employment. If an employer needs to seek consent from their employee, they should do so with a document that clearly states what the consent is being sought for and why, and clearly states that the employee is not obliged to provide consent.

What needs to be done about updating existing employee contracts? Do we need to seek to vary our employees' terms and conditions before issuing updated contracts, or is an amendment enough?

It is not necessary to reissue existing employees with a revised Contract of Employment. Existing employees will be notified of the new Data Protection Act 2018 and the Company's response to it when you issue your Company's new Employee Privacy Notice. You could also enclose your new Data Protection Policy with the Employee Privacy

Notice to be as informative as possible. However, you will need to update your Contract of Employment templates to ensure that your Data Protection clause complies with the Data Protection Act 2018.

If an employee has questions about how their data is used by a third party e.g. a grant company, is it the responsibility of the employer to provide that information, or should the employee seek it separately?

It could be argued that the responsibility falls to all parties. If an employer is sharing employee data with a third party, the employee will need to know exactly what personal data is being shared and why. Part of the "why" will inform the employee how their personal data is being used, but the third party would be in a better position to provide additional details about this. Also, because the third party will be processing the personal data of the employee, they will be required to provide the employer and / or employee with a copy of their privacy notice and confirmation that the data is being processed in line with the Data Protection Act 2018. The privacy notice should provide information on how and why the personal data is being processed. Finally, because the Data Protection Act 2018 acknowledges that personal data is owned by the individual, the employee does have the right to contact the third party directly and ask for information on how and why their personal data is used. In some circumstances this may be the preferred approach, but employers should avoid adopting the attitude of "it's your data, you have to find the answers yourself" because if they're sharing personal data with a third party they should know how it will be used.

If a Company pays for employees to have training, does the associated certificate remain the Company's property or is it the property of the employee?

Even though the Company pays for the training / qualification, from a HR perspective the certificate / qualification is the property of the employee, not the Company. Yes, the Company pays for the training, but it is the employee who completes the training and "earns" the certificate. It is also the employee's personal data that is on the certificate, which makes it theirs. Employees should be given copies of their certificates, and any employer copies should be managed in line with the Data Protection Act 2018.

Are we still ok to monitor employee online activity, and how long can we keep these records?

Employers are still able to monitor employee online activity if this can be justified as a legitimate business need, e.g. the need to manage employee performance and ensure that employees are using time effectively and/or complying with Company policies. It is advisable to seek employee consent to continue monitoring their internet use in this way, and when employers seek consent they will need to clearly explain why they want to collect this personal data, what they will do with it, and when it will be deleted. If this data processing is not carried out for a legal obligation or for the performance of a contract, employers will need to be realistic when considering how long they will retain this personal data for. When managing employees, it is important to remember that they should only be managed for recent or on-going issues; this type of personal data will not be something that should be kept indefinitely. We would advise employers to keep this personal data for six months, or twelve at the very most. After that, it should be destroyed securely in line with the Data Protection Act 2018.

Can you have more than one Data Protection Officer?

The new data protection legislation clearly states that an organisation must appoint a single Data Protection Officer (DPO) to carry out the tasks required in Article 39 of the Act, but this doesn't prevent organisations from appointing other data protection specialists as part of a team to help support their DPO. If you have a team, you should clearly set out the roles and responsibilities of each member, ensuring there is an individual designated as the DPO for the purposes of data protection, and this person must meet the requirements set out in Articles 37-39 of the Act.

What is the likelihood of being audited under the new Data Protection legislation?

The ICO website confirms that they carry out audits on both public and private companies, public authorities and government departments. The ICO chooses to focus on areas where they feel an audit is likely to have "the biggest impact", and they also respond to audit requests. The ICO considers audits to be most suitable for larger companies who process a large amount of personal data. Therefore, audits are possible, but they are less likely for a smaller organisation unless they have been specifically requested, or unless a formal complaint has been lodged with the ICO. However, organisations will still need to be able to easily demonstrate compliance in case they do receive a surprise audit as this is always a possibility.

What defines a Data Breach?

The ICO states that "a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes accidental or deliberate breaches. It also means that a breach is more than just about losing data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the personal data or passes it on without proper authorisation; or if the personal data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed." Information on what to do in the event of a data breach can be found on the ICO website.

Do I need a Data Retention Policy?

When we consider the data protection principles, retention periods are going to be variable unless they are specified in law. The amount of time organisations will retain personal data for will vary depending upon industry, the size of the Company, the type of personal data that is collected, etc. Because of this, it would be difficult to create a document that would specify exactly how long each piece of personal data is retained for, unless this document was created with a lot of caveats that allowed for multiple circumstances. It would not be incorrect to create a Data Retention Policy that communicated how long documentation may be retained, or one that communicated the personal data that needs to be retained for a legally specified length of time, but employees should already be informed of this within the Company's Employee Privacy Notice. Employers should also be wary of the mindset of keeping an employee's personal data for a set amount of time without questioning the necessity of this, as necessity is heavily stressed in the Data Protection Act 2018.

Do historical emails that contain employee data now need to be deleted?

There is no specific guidance from the GDPR relating to emails, and therefore emails will need to be managed in line with the data protection principles. This means that emails need to be held securely and any emails containing employee personal data should only be retained for as long as is necessary. Emails should be audited regularly and destroyed securely in line with the Data Protection Act 2018 when required. There may be some instances in which an organisation has a legitimate reason for keeping emails for a long time, if this is the case consideration will need to be given to how these emails are stored and managed, to reduce the risk of any personal data breaches. It may be that an archiving system should be implemented, where emails can be recovered when necessary but are otherwise unavailable.

Can we anonymise personal data instead of deleting it?

Personal data that has been truly anonymised can be retained indefinitely. However, for the personal data to be truly anonymous it cannot identify or be linked to a data subject in any way. The ICO does not consider any personal data that has been pseudonymised (e.g. key coded etc.) to be anonymous because if the “code” were broken the data subject could be identified. Therefore, if an employer wants to anonymise an employee’s personal data they need to ensure they are doing this in a way that would be legally compliant with the Data Protection Act 2018 for the purposes of data retention.

When does the Right to Restrict Processing apply? Can employees ask for all of their data to be restricted?

The Right to Restrict Processing is not an absolute right, it only applies in the following circumstances:

- An employee contests the accuracy of their personal data and therefore it needs to be verified
- The employee opposes to their personal data being deleted, and wants it to be restricted instead
- The personal data is not required for processing, but may be required by either party to establish, exercise or defend a potential legal claim
- An employee has withdrawn their consent or asked for their personal data to be erased and the employer is considering the appropriate course of action / considering whether their legitimate grounds of processing override the employee’s request

If none of the above points apply, the personal data does not need to be restricted. Not all personal data can be restricted because there may be an overriding legitimate business interest that permits processing e.g. an employee’s bank information cannot be restricted because this would leave their employer unable to pay them.

Do we need to comply with the Right to Data Portability?

The Right to Data Portability gives employees the right to receive their personal data in a structured, commonly used and machine-readable format. Employees can also request that their data is transmitted directly, from one Data Controller to another Data Controller. Because this is a right under the Data Protection Act 2018 (and GDPR), it does need to be complied with, but it only applies in the following circumstances:

- When the lawful basis for processing the personal data is ‘consent’ or for the ‘performance of a contract’; and
- The data processing is being carried out by automated means (i.e. digital means only)

Do the new enhanced rights in relation to Automated Decision Making apply to all Automated Decision Making, or only some aspects?

The enhanced rights in relation to Automated Decision Making, which are detailed on the ICO website, only apply when the Automated Decision Making can have a legal or similarly significant effect on the data subject. If this does not apply to your Automated Decision Making, you will still need to manage the personal data you collect and process in line with the Data Protection Act 2018, but you do not need to worry about the enhanced regulations around this type of data processing.

Is there any protection in place to help employers or companies protect themselves from vexatious subject access requests?

The ICO does not provide guidance on how “vexatious” Subject Access Requests should be responded to or dealt with, but it does state that Subject Access Requests can be refused if the request is considered to be manifestly unfounded or excessive. In this situation an employer can either request a fee before the Subject Access Request is completed, or they can refuse to respond to the request. This approach is acceptable if the fee applied is based on the administrative cost of the request, or if the fee / refusal is clearly justified. We would advise any employer to liaise with the ICO directly if they are receiving multiple / “vexatious” requests and would like detailed advice on how to manage the situation.

How Can We Help?

If you have a question on the Data Protection Act 2018 (and GDPR) that wasn’t answered in this newsletter, or if you have a query on any other HR related matter, please don’t hesitate to contact us at hradvice@hasslefreehr.co.uk