May Employment Law Update

GDPR SPECIAL

As there has been a great deal of publicity and hype relating to the General Data Protection Regulation we have dedicated this newsletter wholly to the GDPR – what it really means and providing you with easy to understand information that will hopefully alleviate fears whilst preparing you for what is to come in the arena of Data Protection.

121 is working on updating employee handbooks and if you have not yet received the new version of your employee handbook, containing the new Data Protection Policy, then it will be with you soon.

What is GDPR?

The GDPR (General Data Protection Regulation) is concerned with respecting the rights of individuals when processing their personal information. From an employment perspective this is achieved by being open and honest with employees about the use of information being held about them, and by following good data handling procedures. The regulation is mandatory and all organisations that hold or process personal data must comply.

What is "personal data"?

Personal data is data that relates to an identified or identifiable individual and is:

- processed electronically and/or
- kept in a filing system and /or
- part of an accessible record, for example an education record and/ or
- held by a public authority

This includes data that does not name an individual but could potentially identify them - for example a payroll or staff number.

What are your responsibilities as an employer?

Employers should ensure that all staff are aware that any personal data they might have in their possession is relevant for the purposes of the GDPR. So if a manager has contact details for their team or an employee keeps customer names and numbers on post-it notes on their desk or on a white board in an open office, this is "data" and is therefore relevant under the GDPR.

The six principles of the GDPR

- Personal data should be processed fairly, lawfully and in a transparent manner
- Data should be obtained for specified and lawful purposes and not used for any purpose other than the reason for which it was obtained in the first place
- The data should be adequate, relevant and not excessive
- The data should be accurate and where necessary kept up to date

- Data should not be kept for longer than necessary
- Data should be kept secure

All staff have a responsibility to ensure that their activities comply with the data protection principles. **Line managers** have responsibility for the personal data they collect and how they use it. **Staff should not** disclose personal data to anyone other than the people in the organisation who may need to use it, or use others' personal data for their own purposes.

In terms of reassurance, if you are already complying with sound data protection policies, then you are well on your way to being compliant with the new regulation!

Monitoring employees

If employers are monitoring their staff, for example to detect crime or wrongdoing, they are required to make their workers aware of the nature and reason for the monitoring. This is applicable whether the monitoring is taking place using CCTV, accessing a worker's email or telephone calls or in any other way. This would be the case in any disciplinary investigation, however – in that an employer is obliged to include a copy of any evidence that has been used to determine the need for a disciplinary hearing.

How long can information be kept?

Information must not be kept for longer than is necessary. While there is no set period of time set out within the GDPR, some records must be kept for a certain period of time in accordance with other legislation. For example, HMRC requirements relating to payroll records.

How can employers comply with the regulation?

To ensure its compliance to the GDPR, an organisation must:

- have a clear retention policy for handling personal data and ensure it is not held for longer than is necessary. **This subject is covered in your annual 121 HR Review process and we make sure we check this with you. Retention guidelines are detailed below.**
- have a legal basis for acquiring and/or using any personal data. **You are entitled to ask for employees' personal details for the purposes of employing and paying them!**
- ensure that all staff are aware of the retention policy and follow it. **This means alerting them to the updated copy of the employee handbook and asking them to sign a declaration like the one below.**
- respond to subject access requests (sometimes called personal data requests) within one month. **121 advise that if you receive a subject access request, you contact us for assistance.**
- if there is a personal data breach that is likely to result in a risk to the rights and freedom of an individual, inform the ICO within 72 hours and, if the risk is deemed to be high, also inform the individual concerned. **The ICO have issued guidance that suggests that if employers alert them early, to potential data breaches, they will provide assistance and support. They are more likely to be punitive is the business avoids alerting them, or tries to hide a potential breach.**

If you have more than 250 employees or process large amounts of data (so if you are working in particular industries where you are processing multiple types of data) you will also be required to appoint a Data Protection Officer who can help embed, communicate and monitor the organisation's GDPR data protection policy.

A worker's right to request their personal data

Workers have a right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.

If you do not already have a privacy statement on your website, an example of a suitable privacy statement is below. If you send out information to clients, you may wish to include it with any information being sent out that links to or requires you to access their data:

We process personal information for certain legitimate business purposes which include, some or all, of the following:

Where the processing enables us to enhance, modify, personalise or otherwise improve our services/communications for the benefit of the customer.

- ***To identify and prevent fraud.***
- ***To enhance the security of our networks and information systems.***
- ***To better understand how people, interact with our social media and web sites.***
- ***To provide postal communications which we think will be of benefit and interest to you.***
- ***To determine the effectiveness of our promotional campaigns and our advertising.***

Whenever we process data for these purposes we will ensure that we always keep your Personal Data rights in the highest regard and take into account all of your data protection right under any and all current UK legislation.

You have the right to object to this processing at any time. If you wish to do so, please click here <link to your opt-out page or to an email address>. Please bear in mind that if you object, this may affect our ability to carry out the tasks above which may be of benefit to you.

Safe Storage of Data

The GDPR places a duty on businesses to ensure that data is maintained securely and that the business has taken adequate steps to prevent cyber-crime. The checklist below is a useful checklist to ask employees to sign, to ensure that they are aware of and take seriously, their responsibilities in this regard:

CHECKLIST: Safe Storage of Information

I acknowledge and agree that:

- I keep my passwords secure. I change my passwords on a regular basis and they are a combination of numbers, letters and symbols. I never share my passwords or write them down on paper.
- I ensure that when my computer is not in use, it is electronically locked. I understand that leaving my computer open and unattended is presenting itself for a potential data breach to occur. I try to log off from my computer when not in use.
- I shred any personal data that is no longer in use or dispose of it in a confidential waste bin.
- I am vigilant when opening emails from unknown senders. The same applies when I visit websites, as not doing this can cause the introduction of viruses and other potential harmful malware into my organisation.
- I adopt a clear desk policy and ensure that at the end of the day, my desk is cleared of confidential information and the information is securely locked away.
- I ensure that any visitors visiting our premises sign in and out and, while on our premises, they are accompanied in areas normally restricted to employees only.
- I try to point my computer screen away from windows to prevent accidental disclosures of personal information. If this is not possible, I ensure that I fit my screen with a privacy attachment.
- I encrypt all personal information that is being removed from my office as it will cause damage or distress if lost or stolen, both to my organisation and the data subjects who have been affected. Furthermore, I risk not only the possibility of brand damage to my organisation but potential penalties that could be levied upon my company by the ICO.

Signed: **Date:**

Similarly, you may wish to ask employees dealing with client data to complete the following declaration:

CHECKLIST: Meeting Customers' and Employees' Privacy Expectations

I acknowledge and agree that:

- I only collect personal information that is required for a legitimate and specific business purpose.
- I have the ability and understanding to explain new or changed business processes, policies and procedures to our customers and employees, and obtain consent or provide an opt out, where appropriate.
- I have the ability and understanding when it comes to ensuring that any personal data I hold is kept fully updated, for example, a change of address.
- I have the ability and understanding to know when it is appropriate to delete personal information that my business no longer requires.
- I understand that I commit an offence if I release customer/employee records without either the company's or the data subject's consent.
- I am aware of any workplace monitoring that may be in operation, for example, through the visible notices displayed throughout my organisation.

Signed: **Date:**

The Right to Erasure (Right to be Forgotten)

The GDPR brings in a new entitlement – namely the right to erasure. This does not provide an absolute 'right to be forgotten' however; individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR)
- The personal data has to be erased in order to comply with a legal obligation

In an employment context this might arise with a "spent" written warning. However there is an argument that suggests that, despite a written warning having expired, it may be retained by the employer in order to inform future disciplinary situations – so "in order to comply with a legal obligation". Like many things, this will be determined by case law going forward. There is no doubt that warnings and disciplinary information will have to be retained securely in order to ensure that it is only accessed when and if needed and not just randomly with someone flicking through an employee file!

When can a request for erasure be refused?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or the exercise or defence of legal claims

This is a whistle-stop tour of GDPR but please do feel that you can contact your account manager by email or contact training@scottishwholesale.co.uk or 0800 9995 121 if you wish to discuss any of this content in more detail.