Call: 078994 25916 / 01295 788 579
e: carole@hrsupportforbusiness.co.uk

HR Support for Business
*A simple and affordable solution to HR*

# HR Micro Guide - GDPR February 2018

**Hello, I'm Carole Thomson and I founded HR Support for Business to give small and medium businesses access to a trusted and flexible senior HR resource when their business needed it. I hope you find this brief overview of the new GDPR useful. Any queries, or if I can help you, please just give me a call.**
**Regards Carole**

## Processing employee data under the GDPR

Reported as being the most comprehensive evolution of data protection rights in 20 years, the new EU Data Protection Regulation (The General Data Protection Regulation or GDPR) will come into force for EU member states on 25 May 2018. Key changes include: a wider definition of personal data; different requirements in how data controllers and processors need to manage personal data; tighter rules around consent and wider data user rights. Basically, almost all personal information about any individual will be protected (and will fall under this regulation) if they can be identified by it in some way. It also reflects the many changes in technology and the way businesses collect and use information about people.

It also brings additional hurdles regarding "special categories of personal data" which is a similar, but a slightly broader, version of what is currently known as "sensitive personal data". This will cover information relating to employees' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information and data relating to sex life and sexual orientation. As well as lawful basis (see below) for processing such data you will need to meet at least one further condition for processing 'special category data'.

The fact is that the GDPR will apply to every business, of every size, across every function where personal data is collected, stored and used. So, not just a HR thing. However, in the context of HR, it will include the personal data of: job applicants; employees; workers and consultants across the lifecycle of their working relationship with you. And, will Brexit change anything? The Information Commissioners office (ICO) guidance says no.

**And, of course, it brings increased penalties should you get it wrong.** Penalties for serious non-compliance bring a maximum fine of the greater of 4% of worldwide turnover, or up to 20million. Smaller offences could result in fines of the greater of 2% of worldwide turnover or up to 10million. And they have the power to suspend a business from using the data. Not something any business can afford to ignore

## So first, let us look at the legal basis for processing personal data

A key principle underpinning the GDPR is that personal data must be "*processed lawfully, fairly and in a transparent manner in relation to individuals*". So, it is essential that you first identify exactly what data you are processing, why and the lawful basis you are relying on. Just looking within the employment context, it

is most likely going to be:

- You have a data subject's consent;
- you need to process the data for the performance of the employment contract;
- you need to process the data to comply with a legal obligation you must comply with;
- processing is necessary for the purposes of the legitimate interests pursued by you or a third party (except where overridden by the interests, rights or freedoms of the data subject);
- protecting the vital interests of the data subject, or of another person, or a necessity for the performance of a task carried out in the public interest.

**Consent – the problems and the pitfalls.** The first problem is that the ICO consider consent as problematic. They consider an employee cannot be on an equal footing with their employer – so how can there be a real free choice? How can consent be freely given with such an '*imbalance of power'*. And therefore, how can it meet the GDPRs new, tighter, definition of consent, which is: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

Second, consent must be as easy to withdraw as it was to give it (made very clear at the outset), and if consent is withdrawn this could be problematic for employers. Also, as consent must be separate from other terms and conditions the current popular 'catch all' consent clause widely used within a contractual terms and conditions of employment will not meet the new requirements. And remember, there is a clear difference between telling a person how you propose to use information '*lawful basis'* and getting their consent to process it. If consent is needed the current draft guidance requires:

- consent is a positive action, an 'opt in', a free choice, separate from other terms and conditions, and not passive relying on silence, or an inactivity on the part of the data subject;
- consent is gained for the specific data in question and the reason given for you using it;
- it must be clear, not vague or ambiguous and in plain language;
- transparency whether you intend to share the information - so who, why (e.g. outsourcing);
- it is made clear they have the right to withdraw consent and how they can easily do this;
- you refresh any consent ensuring you maintain up to date data records.

Plus, if you need to transfer data outside of the EU there are further requirements you must satisfy (e.g. gain explicit consent for this purpose, or to enter the EU standard contractual clauses).

And for anyone thinking they could initially get consent, then rely on a lawful basis if the "consent" is withdrawn, think again. The ICO have made it quite clear they intend to discourage this type of behaviour. Basically, they consider it would be "*misleading and inherently unfair"* giving only the "illusion" of control.

However, the good news is that it would appear most routine employment processing activities will naturally fall under one of the 'other lawful purposes' (above). You just need to identify which *'lawful purpose'* for the personal data in question and how you want to use it and retain it. And be careful, the new Accountability principles (see below) require you to be able to demonstrate an audit trail to ensure your compliance to this, so you cannot then use any data for a different purpose than initially identified.

**Special category data**. Finally, when looking at this area it is generally advised to avoid relying on consent if possible and identify another legitimate basis for processing. Alternative conditions for such data include:

- to perform or exercise obligations or rights of the employer, or employee under employment law, such as not to discriminate against an employee or dismiss them unfairly;

- to establish, exercise or defend legal claims; or
- to assess an employee's working capacity, subject to confidentiality safeguards.

## The GDPR also brings new 'principles' – notably:

**Accountability and transparency**. Emphasising the need for a business to not only comply with the GDPR, but also to be able to demonstrate an audit trail on how they comply. Integral is the need to build in a greater emphasis on privacy by design and default across a business. So, privacy considerations are an integral element of all systems and procedures (with the intention of making breaches, whether large or small, more unlikely). Anyone who has undertaken a risk assessment will understand this principle of identifying risk and risk reduction by design - and this must be documented – for transparency.

**Data minimisation' or storage limitation'**. You are now required to build into your systems and procedures how you will proactively reduce the overall personal data you collect, process and retain as a business. Limiting personal data within your business to only what is necessary for the purpose(s) for which the data was first obtained. And, ensuring you have a system to ensure no data is kept for longer than is necessary (without a clear reason or justification).

So how long is too long? This will depend on the nature of the information you are processing and your justification (lawful purpose) or the limitations of the consent. You will however, be required to review and update your data retention and deletion practices.

## And, the GDPR also brings new individual rights – notably:

**Right to be informed.** As an example your workers will have the right to be informed about: what data (categories) you require; the lawful purpose you are relying on for processing the data; how it will be used; details of the Data Controller; if data is to be transferred or shared (specifically if outside the EU), and with whom; what safeguards are in place; how long data will be held and how do you anticipate storing the data; a list of their rights under GDPR; if consent is needed their right to withdraw consent at any time and how to do this; how to raise a concern and if they will be subject to any automated decision making.

**The right of access to information remains**. But with a key change, as you must now respond to a Subject Access Request (SAR) 'without delay' and at the most within one month (currently 40 days to respond). Guidance does say this may be extended by a further two months if complex (but no real detail on exactly what would be accepted as complex). And, it must now be provided free of charge, unless the request is repetitive or unfounded (again no great information of exactly what would be accepted).

**Right to rectify**. These rights require you to rectify the information you hold internally, or shared/held externally with no need for a court application. And you must respond within a month.

**Right to erasure or the right to be forgotten.** Meaning just that. The right to require the deletion of personal data where the data is no longer necessary for the purpose which it was originally collected. Or, where consent has been withdrawn and you, the employer, has relied on the employee's consent to process that personal data, or the personal data was processed in breach of the GDPR.

**Right to data portability.** Allowing individuals to acquire their personal data in a structured, commonly used/IT readable format – of course at no charge, enabling the safe and secure transportation of data.

**Right to object.** Individuals will have the right to object to processing in certain circumstances. Even where it has been based on a lawful purpose. If an objection is raised you must stop the processing until you can demonstrate compelling legitimate grounds for the processing which override the interest, rights and freedoms of the individual, or can show that processing is necessary in connection with legal proceedings.

**Right to be informed of automated decision making and profiling** This is only a brief overview of the wider GDPR requirement to provide protection to individuals against the potentially damaging decisions made without human intervention. As an overview it gives individuals the right to be informed and the right not to be subject to any decision based automated processing where it produces a legal or similarly significant effect on the individual. You must also ensure that individuals are able to: obtain human intervention; express their point of view; and obtain an explanation of the decision and challenge it. It does not apply to all automated decisions and the GDPR defines profiling as "*any form of automated processing intended to evaluate certain personal aspects of an individual, in particular, to analyse or predict*". They give a range of examples, but to give you an idea one listed is: to asses an individual's performance at work.

## And there are new rules regarding a data breach

The GDPR requires that any data breach is reported 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. For instance: 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: 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. The short timescale for reporting, means you need to have a procedure (response plan) in place for such an occurrence, to ensure that the breach could be identified, reviewed and reported in time.

## So, what should you do now?

This is a long legislation, and (even at 5 pages) this is still just a brief overview highlighting some of the factors I feel are key. Of course, if you need any help with anything then please just call**.** But as a general overview, these are the initial actions I would recommend:

**You first need to identify where you are now**. You need to undertake a data audit (or data mapping). The scope of your audit should include all HR personal data held in electronic format or contained within a structured manual filing system across your workforce. You will also need to consider data stored or processed outside of HR (external third party or host) and internally (Finance).

The sort of things you need to identify are: what personal data do you currently collect? Why and how do you use it? How long do you retain it? Who has access? Do you rely on a 'lawful basis' (see above) or consent? How is this communicated or obtained? How do you communicate an individual's rights? And so on, recording exactly what you are doing now and evaluating if it meets the new GDPR requirements or not? This will identify what you need to do - pinpointing gaps or actions needed.

Once you have this information I would then recommend you:

- review and, if needed, amend your contract templates to comply with the GDPR;

- develop stand-alone privacy notices. These seem to be the most recommended and acceptable route to inform new and existing employee of the specific types of employee data you wish to collect and the justification (lawful purpose) you are relying on etc;
- amend your data protection policy/procedure to reflect new rights under the GDPR, and how you will comply with the GDPR;
- review and amend other procedures within your handbook, for instance recruitment and selection;
- where consent has been identified as needed, create a separate document to be able to gain consent and comply with the GDPR and;
- whilst there is no need to automatically refresh all existing DPA consents, you will need to review if they comply with GDPR requirements, or if it is more appropriate to rely on a lawful purpose;
- review any template documents that collect data – Do they comply?
- Agree how you are going to communicate this and make a plan.

But, of course these are just examples. Once the audit is completed you may identify other actions bespoke to your business as you go along.

Finally, this new legislation is very long, and as I mentioned, even at 5 pages (I tried to keep it shorter – I promise!), I can only endeavour to give you a brief guide, or an overview. It cannot cover everything held within this new legislation, and it cannot constitute legal advice or a legal analysis. It is just an overview from a HR point of view to highlight (if you do not already know) that the General Data Protection Regulation is coming soon, and it will apply directly to your business.

The responsibility to read and become familiar with the Regulation and comply with its provisions from 25th May 2018 onwards therefore lies with each individual business. And hopefully there is more guidance from the Government on its way.

But I hope it will at least help with this task and of course, as I have already mentioned, I am happy to help you will any stage of the process you only need to ask.

Regards

*Carole*

Carole Thomson – Senior Freelance HR Consultant FCIPD, TechIOSH
HR Support for Business
T: 01295 788 579 M: 07899 425916
E: carole@hrsfb.co.uk
www.hrsupportforbusiness.co.uk

 