Gregg Latchams Solicitors

# Supplemental guide to the GDPR for HR professionals

Version 1.0, January 2018

**The General Data Protection Regulation (GDPR) will come into force on 25 May 2018, representing the most significant change to European data protection law in over 20 years. For a general overview, we have written 'A Practical Guide to the GDPR'. In this supplemental guide, we take look at the impact of the GDPR from an HR perspective.**

## Contents

## Introduction

From recruitment to retirement and everything in between, employers often process more personal data about prospective, current and former employees than they realise.

In addition to general biographic and payroll data, such personal data may include:

- Application forms and CVs
- CCTV footage and building access data
- Computer and other device usage
- Disciplinaries and grievances
- Health and other medical information
- Performance reviews (appraisals)
- Protected characteristic information
- Telephone call records and recordings
- Training and testing outcomes
- Trade union membership details

The way in which processing obligations are framed under the GDPR requires employers to take a more proactive approach. The GDPR also enhances and extends the rights of employees in relation to the processing of their personal data and introduces potentially significant penalties and enforcement measures for employers if they get it wrong.

There is an opportunity for HR professionals to play a leading role in assisting employers with their compliance obligations in the employment context. In particular risk management, policy implementation and staff training are important skills that HR professionals can leverage in creating a 'compliance culture' with their organisations.

**ACTION:** If you don't know what personal data you hold about employees, start with a 'data mapping exercise'. This could be as simple as a spreadsheet which identifies the types of data being held, the format they are held in, the purposes for which they are processed, who has access, where they are held and with whom they are shared. There are also products on the market that can help with undertaking this exercise.

## Accountability

The need to take a more proactive approach derives from the accountability principle, which not only requires employers to comply with the core principles of the GDPR but be able to *demonstrate* compliance with those principles. For an employer, this means being able to show that employee personal data are:

1. **Processed lawfully, fairly and in a transparent manner:** employers must ensure that one of the conditions for lawful processing are met (see **Lawful grounds for processing** below) and that they are clear and transparent with employees about the purposes for which their personal data are processed, both at the time of collecting it and when any changes to such processing are proposed;

2. **Only processed for specified, explicit and legitimate purposes:** employees' personal data must not be used for any purposes that are incompatible with those for which the personal data were originally collected. Whether any new purpose will be compatible requires careful assessment taking into account a number of factors including the link between the original purpose(s) and the further purpose(s);

3. **Adequate, relevant and limited to what is necessary:** employers should not collect more personal data about employees than is necessary for each of the specific purposes that it has identified to its employees. Complying with this principle enables compliance with a number of the other principles and requirements of the GDPR;

4. **Accurate and kept up-to-date:** employers must ensure that employees' records are accurate and up-to-date. The GDPR requires employers to "take every reasonable step" to ensure that inaccurate personal data are corrected or deleted "without delay";

5. **Not kept longer than necessary:** subject to a few exceptions, employers must not keep employees' personal data for longer than is necessary in connection with the purposes for which such data were collected. Employers will need to consider the retention periods for each category of employee personal data they hold and have a system in place for purging records following expiry of those periods;

6. **Processed in a manner that ensures they are kept secure:** employers must use "appropriate technical or organisational measures" to protect personal data from unauthorised or unlawful processing and against accidental loss, destruction or damage. Employers should consider who should have access to each category of employee personal data, where the data are stored and whether the data are secure.

**ACTION:** Review each category of personal data against each of the above principles and document how you intend to implement and demonstrate compliance with those principles. Remember that you should only process the minimum amount of personal data necessary to achieve each purpose.

## Lawful grounds for processing

In order to process personal data, an organisation must have a lawful basis for doing so. Historically, employers have relied heavily upon consent from employees through getting them to sign an employment contract which contains a generic "catch all" data protection clause or a separate consent form.

Under the GDPR, consent is unlikely to form a valid ground for processing employees' personal data except in circumstances where the employee can be said to have a genuine choice (for example, the sharing of their personal data with an employee benefits provider). The GDPR makes it clear that consent cannot be "freely given" where there is a clear imbalance in the relationship between a controller and a data subject, such as that between an employer and employee. Furthermore the GDPR provides that:

- Consent to the processing of personal data should be 'unbundled' from any other contractual terms, such as the terms of an employment contract;
- Consent must be 'granular', meaning that it must be possible for an employee to consent to some processing activities and not others rather than giving sweeping consent; and
- Consent must be as easy to withdraw as it was to give in the first place.

As such, employers will have to consider whether they have an alternative legal ground for processing employees' personal data in respect of each purpose for which they are processed. The three most relevant grounds are:

1. **Where the processing is necessary for the performance of a contract:** The most obvious example is the processing of an employee's bank details in order to pay their wages and provide other contractual entitlements;

2. **Where the processing is necessary in order to comply with a legal obligation:** Employers will need to maintain records of sick leave and other types of leave for which statutory payments are available, as well as complying with health and safety law in certain circumstances;

3. **Where the processing is necessary for the employer's legitimate interests:** This ground enables an employer to process an employee's personal data where it has a legitimate interest (more than simply an economic interest) which is not outweighed by an employee's right to privacy (see Employee monitoring below) and such processing is necessary in pursuing that interest. Relying on this ground requires a careful assessment.

**ACTION:** Consider the most appropriate lawful basis for processing each category of employee personal data. If you wish to rely on legitimate interests, you should undertake a 'legitimate interest assessment' (the Data Protection Network has produced a helpful guide on this – registration required). Once you have completed this process, you should review your employment contracts, staff handbook, policies and other fair processing notices to ensure that they communicate the information required by the GDPR, including a description of the lawful grounds relied upon.

## Special category data

The GDPR prohibits the processing of 'special category data' (previously called 'sensitive personal data', but now including general 'health data', data about sexual orientation and 'biometric data' and 'genetic data') except in certain circumstances. The most relevant conditions from an employer's perspective are:

1. **Where the employee has given their 'explicit' consent:** Although 'explicit' is not defined, it is understood that this is a higher standard than 'unambiguous': there must be no room for misinterpretation, therefore a clear oral or written statement will be required;

2. **Where the processing is necessary in connection with the employer's or employee's obligations in the employment context:** although a similar exception existed under the Data Protection Act 1998, the rules are now much stricter. The draft UK Data Protection Bill (**DPB**) which will formally repeal the 1998 Act and supplement the GDPR when it comes into force) provides that employers must:

   - have an "appropriate policy document" in place explaining how it will process such data in accordance with the GDPR's principles, including an indication of how long it is likely to be retained and how it will be erased;
   - ensure that the policy is reviewed and updated as appropriate, made available to the ICO on request without charge and retained for a period of six months beginning with day on which the employer ceases to process such data; and
   - maintain a record of its processing of such data, including the condition relied upon by the employer (most likely one of the three noted in the section above) and whether such data has been processed in accordance with the policy.

   Examples of processing special category data on the basis of this ground include:

   - Checking the entitlement of workers to work in the UK;
   - Ensuring a safe working environment for all workers;
   - Maintaining records of statutory sick pay and other statutory entitlements;
   - Disclosing accident records in the context of a personal injury claim;
   - Protecting an employer's or customer's property or funds;
   - Providing employee liability information to a potential buyer under TUPE.

3. **Where the processing is necessary for the performance of a task carried out in the 'public interest':** the draft DPB prescribes which tasks are considered to be in the public interest, the most relevant being:

- the processing of personal data revealing racial or ethnic origin or religious or philosophical beliefs, data concerning health and personal data concerning an individual's sexual orientation, in each case for the purposes of monitoring the existence or absence of equality of opportunity or treatment between groups of individuals;
- the processing is necessary to determine eligibility for or benefits payable under an occupational pension scheme and such processing can reasonably be carried out without the individual's consent being obtained.

4. **Where the processing is necessary for the assessment of the working capacity of an employee:** specifically, this ground relates to an individual's working capacity on health grounds, subject to appropriate confidentiality safeguards being put in place.

Other conditions that are less likely arise during day-to-day operations include processing in relation to the prevention or detection of unlawful acts, processing in relation to bringing or defending legal claims or to protect an employee's or someone else's interests (where consent would not be appropriate) or where an employee has already "manifestly made" such data public.

**ACTION:** Having identified the extent to which your organisation processes special category data, you will need to consider and document which condition for processing such data applies. Where processing is deemed necessary for the purposes of carrying out employment law rights and obligations, you will need to ensure that you have an appropriate policy in place and a procedure for retaining and reviewing such policy.

### Criminal convictions and offences data

Personal data relating to criminal convictions and offences includes personal data relating to the alleged commission of offences by an individual, proceedings for an offence committed or alleged to have been committed by an individual or the disposal of such proceedings (including sentencing).

The GDPR prohibits the processing of personal data relating to criminal convictions and offences unless authorised by law. The draft DPB provides that an employer may process such personal data where necessary under employment law or where there is a substantial public interest in doing so (see the above requirements for special category data, which are essentially mirrored). In addition, an employer can process such personal data if one of the following conditions is met:

- the employee has given their consent;

- the processing is necessary to protect the "vital interests" of an individual and the employee is physically or legally incapable of giving consent;
- the processing is carried out in the course of the legitimate activities of a not-for-profit body which has a political, philosophical, religious or trade union aim, subject to appropriate safeguards being put in place;
- the employee has already "manifestly made" such data public; or
- the processing is necessary to establish, bring or defend a legal claim.

**ACTION:** Review fair processing notices for job applicants and employees to identify whether the relevant conditions for processing criminal convictions and offences data are clear. Prepare a policy for the processing of such data and, where relevant, ensure that there is an appropriate consent form for processing such data.

## Recruitment and selection

According to a YouGov survey (April 2017), one in five UK employers have turned down a candidate after checking their online activity. Employers often assume that anything they can find out about a candidate online can fairly be used to evaluate them offline. However this is not the case: viewing a candidate's social media profile as part of a recruitment process constitutes 'processing' ("retrieval, consultation or use") and one of the legal grounds for processing will therefore need to be met.

As the GDPR makes it clear that consent cannot be relied upon where there is a "clear imbalance" between a data subject (such as a job candidate) and a controller (such as a prospective employer), an employer would need to show that it has a legitimate interest in the processing which outweighs a candidate's right to privacy.

Guidance issued by European data protection advisory body, the Article 29 Working Party (**WP29**), suggests that in making such assessment, an employer will need to take into account whether any social media profile was established for business or personal purposes and whether such processing is *necessary* and *relevant* to the performance of the job being applied for. This may be easier for regulated professions, where 'character and suitability' are important factors to be taken into account.

The Employment Practices Code published by the Information Commissioner's Office (**ICO**) also provides that the sources of information that might be used by an employer as part of any recruitment process should be explained in any job advertisement or application form.

**ACTION:** Establish a policy for recruitment and selection which sets out your organisation's requirements in relation to vetting. Reflect your data processing activities in the context of recruitment and selection in a 'fair processing notice' for job applicants which can be found by candidates easily at the point of application.

## Workplace monitoring

There are a number of legitimate reasons why an employer may want to implement workplace monitoring, whether through monitoring emails, internet traffic or telephone use or through CCTV and other physical surveillance methods. It has been clear for some time that employees have a reasonable expectation of privacy in the workplace and that this right needs to be carefully balanced against an employer's interests.

The GDPR does not specifically address workplace monitoring nor does it substantially change the general position under the 1998 Act, which is that employers must have a fair and lawful basis for processing personal data in the context of workplace monitoring which must be clearly communicated to employees beforehand.

The Employment Practices Code published by the ICO recommended that employers undertake an impact assessment to identify any adverse impact of workplace monitoring and to help decide whether they should proceed. However it is likely that workplace monitoring would be considered "high risk" processing for the purposes of the GDPR, given that it will generally involve "a systematic and extensive evaluation of personal aspects…which is based on automated processing". As such, the GDPR will require employers to undertake a mandatory Data Protection Impact Assessment (**DPIA**) to identify the risks and how those risks may be mitigated. If the result of the DPIA is that the identified risks cannot be effectively mitigated, the GDPR will require the employer to consult with the ICO before implementation.

Guidance on data processing at work published by WP29 notes in particular that:

- the use of technologies for keystroke logging, tracking mouse movements, enabling webcam access or screen capturing are likely to be disproportionate and unlawful in most circumstances;
- the use of vehicle telematics to collect data about an employee's location and driving behaviour for performance management purposes is likely to be disproportionate and unlawful (except to demonstrate compliance with legal obligations regarding driving time, speed and distance such as tachographs);

**ACTION:** Review your systems and policies for employee monitoring against the recommendations contained in the Employment Practices Code and consider whether they are justifiable and proportionate having regard to your organisation's legitimate interests or legal obligations. If you are considering implementing any form of direct or indirect employee monitoring, undertake a Data Protection Impact Assessment. Where deemed appropriate, consult with employees about any proposed monitoring.

### Bring Your Own Device (BYOD)

There are a number of benefits and risks associated with allowing employees to use their own devices for work purposes. An employer must ensure that it remains in control of any personal data for which it is responsible regardless of who owns the device on which it is accessed, stored or otherwise processed.

In addition to the general requirement to take appropriate technical and organisational measures to protect against a personal data breach, the GDPR provides that an employer, in its capacity as a controller, should have "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing…" As such, employers will need to implement appropriate systems and policies to ensure that it is able to achieve the required standard when personal data are accessible from employees' devices. Employers will also need to consider how they will identify and respond to personal data breaches involving devices owned by their employees.

At the same time, an employer must respect an employee's right to privacy in respect of the use of any device for personal, non-corporate purposes. The use of technologies to collect device identifiers, perform security scans and ultimately erase or lock a device if it has been identified as lost or stolen (known as Mobile Device Management, or MDM), is potentially privacy intrusive. In its Guidance on data processing at work, WP29 recommends that an employer should:

- ensure that it only has access to those sections of a device which are strictly necessary for the purpose of ensuring the security of corporate data (for example, by 'sandboxing' data within a specific app or folder);
- not be able to capture data relating to an employee's private and family life such as real-time location tracking or private photographs and usage data;
- ensure that devices are configured to enable the secure transfer of data between the employee's device and the network (for example, via a VPN connection);
- perform a DPIA where it intends to deploy MDM.

Further guidance on implementing a BYOD strategy can be found in the ICO's BYOD Guidance.

**ACTION:** Review and update any existing BYOD policy to ensure that employees understand the risks associated with the use of their device for work purposes and to take steps to prevent any personal data breaches from occurring. Coordinate with IT to ensure that appropriate technical measures have been implemented and where those measures may have an adverse impact on employees, undertake a DPIA.

## Rights of employees

Subject access

Many employers will be familiar with the right of subject access which gives employees (and any other individual about whom an employer processes personal data) the right to request a copy of their personal data. Often the right is exercised in the context of an employment dispute, as a method of obtaining records that might assist the employee's case.

Under the GDPR there are some subtle yet important changes which will require employers to review their procedures for responding to subject access requests:

- a response to a subject access request (**SAR**) must be provided "without undue delay and at the latest within one month of receipt", though the period may be extended by up to three months if the request is particularly complex;
- if an employer does not respond to a SAR within the required timescales, it must notify the employee of its reasons and the possibility of lodging a complaint with the ICO;
- a response to a SAR must be provided free of charge, unless the SAR is "manifestly unfounded or excessive", in which case the employer may charge a "reasonable fee" or refuse to act on the request (the employer may need to engage with the employee the narrow the scope of their request and will need to be able to justify its position in any case);
- further information must be provided with the response including details of the envisaged period of storage (or criteria used to determine such period), details of the employee's further rights (see below) and details of the safeguards applied by the employer for transferring the personal data outside of the EEA, where applicable.

As with the 1998 Act, the GDPR provides that confidential references given by an employer for employment purposes are exempt from the subject access right. However an employee may still exercise their subject access right against the employer that they applied to even if the reference was given "in confidence" (though that employer will have to consider whether the whole reference should be disclosed, for example, because it clearly identifies the author of the reference).

**ACTION:** Review your procedures for responding to SARs to ensure that they reflect the new requirements. Ensure that appropriate members of staff are trained on how to identify when a SAR has been made and consider how you would respond to a SAR, perhaps by running a trial exercise across business divisions.

Further rights

In addition to the right of subject access, employees will also have the following rights:

- **The right to be informed:** the GDPR requires employees to be provided with significantly more information about how their personal data will be processed and their rights in relation to such processing;

- **The right to rectification:** employees have the right to request that inaccurate personal data held about them are corrected or completed, if incomplete;

- **The right to erasure (to be forgotten):** this gives employees the right to request the deletion of their personal data in certain circumstances, notably when:
  (a) the personal data are no longer necessary for the purposes for which they were collected;
  (b) they withdraw their consent to processing and there is no other legal ground for processing;
  (c) the employee has objected to the processing and there is no overriding legitimate ground for processing by the employer; or
  (d) the personal data have been unlawfully processed (for example, because the employer's fair processing notice is inadequate).

  If exercised, the employer must also "take reasonable steps" to inform third parties that the employee has requested erasure of their personal data;

- **The right to restriction of processing:** employees have the right to restrict the processing of their personal data in certain circumstances, notably when:
  (a) the employee contests the accuracy of their personal data;
  (b) the personal data have been unlawfully processed (instead of requesting erasure);

(c) the employer no longer requires the personal data, but the employee needs the personal data to establish, exercise or defend a legal claim; or

(d) the employee has objected to the processing and is waiting for the employer to verify whether it believes its legitimate grounds for processing override the interests of the employee.

Once the request has been made, the employer may continue to store the personal data, but must not do anything else without the employee's consent or for certain other limited purposes;

- **The right to object to processing:** employees have the right to object to the processing of their personal data in certain circumstances, notably, where their personal data are processed on the basis of the employer's legitimate interests. Once the right has been exercised, the employer must stop processing the personal data unless it can demonstrate that it has "compelling legitimate grounds" for processing the personal data which overrides the employee's interests or it needs to process the personal data to establish, exercise or defend a legal claim;

- **The right to data portability:** employees are entitled to request a copy of their personal data, including personal data provided by them and observed about them, in a "structured, commonly used machine-readable format" (i.e. a format that can be read and processed by a computer) so that they can transfer such data to other organisations;

- **The right not be subject to automated decision-making:** employees have the right not to have decisions made about them which are *solely* determined by some automated process or profile relating to them, where those decisions would have legal consequences for them or "similarly significantly affect them". In an employment context, this could include the use of automated tools during the recruitment and screening process or tools which are used to assess job performance and productivity.

**ACTION:** Review and update your policies and procedures and fair processing notices to ensure that they reflect the extended and enhanced rights under the GDPR. Consider whether and to what extent your organisation is able to comply with each of the rights and document the steps that you will take to adapt your systems accordingly.

## Third party processors

From payroll and employee benefits providers to external HR consultants, it is not uncommon for employers to engage third parties in connection with the administration and management of their employees. Employers may also use cloud-based solutions, for example, to enable employees to view and update their records and undertake training. Each of these organisations will likely be a "processor".

Although processors are now directly subject to obligations and liabilities under the GDPR, draft guidance from the ICO on liabilities between controllers and processors makes it clear that controllers remain "ultimately responsible" and that "unless you can prove that you were not in any way responsible for the event giving rise to the damage, you will be fully liable for any damage caused by non-compliant processing, regardless of your use of a processor".

As such, employers must undertake rigorous due diligence on all third parties involved in processing employee personal data to ensure that they can provide "sufficient guarantees" regarding their ability to implement the GDPR's requirements.

Critically, employers must ensure that they have contracts in place with third party processors that comply with the more stringent requirements of the GDPR. In particular, such agreements must specifically set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects involved and the obligations and rights of the controller. Ensuring that existing and new agreements are updated to reflect these new requirements is likely to be a burdensome task but is essential to demonstrating accountability and mitigating the risks of using third party processors.

Where any personal data relating to employees are to be transferred outside the EEA (which includes using third party services that are hosted outside the EEA), employers must ensure that one of the conditions under the GDPR is met.

**ACTION:** Identify all third party providers involved in processing employee data and review (a) whether they are able to provide sufficient guarantees regarding their ability to process the personal data securely and in accordance with the GDPR's requirements; and (b) all contractual terms with such third parties and take steps to ensure that they are updated.

## Employment records and pseudonymisation

It is clear that the GDPR introduces stronger obligations on employers to maintain processes that ensure good data governance in relation to employment records and respecting the rights and interests of employees. Furthermore, for organisations with 250 or more staff, there is an obligation on employers to maintain specific records of their processing activities both in relation to their employees and any other individuals about whom they process personal data.

The GDPR also introduces the concept of "pseudonymisation", which is defined as the processing of personal data in such a way that they can no longer be attributed to a particular individual without additional information. This is generally achieved by assigning a "code" to each individual that is stored separate from other personal data and is subject to technical and organisational measures that ensure they cannot be attributed to an individual.

Data which has been "pseudonymised" will still be personal data and, as such, will not exempt personal data from the GDPR's requirements. However the GDPR provides a number of benefits and concessions as an incentive to adopt the practice:

- pseudonymised personal data are exempt from an individual's rights to access, rectification, erasure and portability;
- organisations are not required to notify the ICO or individuals of any data breaches involving pseudonymised data provided it has been done properly (i.e. individuals cannot be re-identified from the coded records); and
- pseudonymising personal data is identified as an "appropriate safeguard" which may support an organisation's ability to process personal data for further purposes that are compatible with the purposes for which they were originally collected.

**ACTION:** Consider whether the systems and processes used within your organisation will enable you to comply with the GDPR's core principles and demonstrate compliance with your obligations. Undertake a review of your systems to identify whether records can be pseudonymised and consider establishing a protocol for pseudonymisation.

## Training

Ensuring that all staff engaged in the processing of personal data (whether directly or indirectly) receive initial and ongoing training is essential to demonstrating compliance with the GDPR's requirements and mitigating the risk of human error, which is the most common reason for data protection breaches.

Employers should consider the training needs of different groups of employees based on the nature, complexity and risks associated with their tasks and deliver tailored training programmes that are engaging because they are relevant to their needs. It may also be necessary to provide technical training on how to effectively use IT systems and change settings on personal devices in line with the organisation's BYOD policy (see above). In addition to maintaining training logs, employers may also want to consider using quizzes, 'gamification' and other methods of assessing employees' understanding of the part they have to play in protecting personal data.

**ACTION:** Review the training needs of your staff and develop training programmes that are relevant to them. Think about ways training can be delivered in an engaging way and how understanding can be assessed on an ongoing basis.

# How we can help

If you need specialist advice on any aspects of this guide, our Data Protection team would love to hear from you. Our team is able to assist with:

- Contract Drafting & Reviews
- Cybersecurity Strategy
- Data Protection Audits
- Data Protection Impact Assessments
- Policies & Procedures
- Privacy Notices
- Regulatory Enforcement
- Reputation Management
- Subject Access Requests
- Training

To get in touch:

**Call:** +44(0)117 906 9400
**Email:** enquiries@gregglatchams.com

# Disclaimer

Although we have taken great care in preparing this guide, it is not intended to constitute legal advice on which you should rely. Data protection law is a complex and highly context-specific area of law. We give no warranties of any kind, express or implied, with regard to the accuracy, timeliness or completeness of any information contained in this guide. If you have any questions arising from this guide, please contact the solicitor or other member of staff with whom you usually deal.

# Regulatory Information

Gregg Latchams is a limited company registered in England & Wales (company number 06899567) and is authorised and regulated by the Solicitors Regulation Authority (SRA number 607476). For further information about how we are regulated, please visit the Regulatory Info page on our website.