PENNINGTONS MANCHES

# THE EMPLOYMENT GUIDE TO GDPR

**The General Data Protection Regulation (GDPR) will be expressly implemented into UK law through a new Data Protection Act. This will need to comply with the overhaul of European data protection legislation brought about by the GDPR as a result of the rise in the use of technology information systems and digital media as well as social and legal issues relating to privacy and data use.**

The GDPR will come into force on 25 May 2018 without the need for specific UK legislation. The UK's Data Protection Bill ("the Bill") was published and put before Parliament on Thursday 14 September 2017. The Bill seeks to implement the GDPR in full, covering specific areas which are left to be determined by member states and introducing a GDPR-like regime to aspects of data processing technically not covered by the GDPR itself. Although the Bill may be amended, it is unlikely that there will be material changes and it is important to prepare now. The GDPR applies to organisations with a UK establishment where personal data is processed in the context of the activities of any establishment. If this is met, the GDPR applies irrespective of whether or not the data processing takes place within the EU. Processing means doing anything with data, including sharing and deleting it. In short, all UK employers process the personal data of candidates, employees/workers, former employees/workers and consultants, irrespective of the other activities of the business.

This guidance note applies to all businesses. It can be read alongside more general guidance in respect of preparing for the GDPR but is focused on those within the HR community.

## NEW CONCEPTS

The GDPR introduces significant changes in respect of:

- Regulated data – the definitions of "personal data" and "sensitive data" (now "special category data") have been expanded: for example, genetic and biometric data is now included.
- Consent – the information that must be provided to individuals and the permissions required to justify use of personal data are expanded. Consent to processing must be freely given, unambiguous, and not assumed from inaction. Consent given in an employment contract is not likely to be unambiguous, and there are also difficulties due to a perceived inequality in bargaining power. Relying on consent to justify the processing of employee personal data will be difficult and alternative approaches should be considered.
- New concepts are introduced in respect of pseudonymisation where information which allows data to be attributed to specific people is held separately and subject to technical and organisational measures to ensure non-attribution.

## PERSONAL DATA

The GDPR will apply to data from which any living individual is identified or identifiable (by anyone) whether directly or indirectly. Certain online identification may count as personal data including online ID, cookies and IP addresses. The definition of "special category data" (previously referred to as sensitive personal data) is extended. As with sensitive personal data under the existing Data Protection Act the processing of special category data is subject to more stringent conditions than other forms of data.

PENNINGTONS MANCHES

## DATA MAPPING

The data protection principles have been revised although they are broadly similar to those in the current Data Protection Act. They cover:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- data quality
- security
- integrity
- confidentiality

A new data protection principle makes data controllers (in other words, employers operating HR systems) responsible for demonstrating compliance with the Data Protection Principles. This is the principle of accountability which flows through the GDPR.

### Actions

Data protection policies, codes of conduct and training need to be reviewed to ensure these are consistent with the revised principles and more stringent rules. Terms in employment contracts will need to be considered and potentially amended. Companies will need to identify means to "demonstrate compliance". This will involve considering codes of conduct, paper trails of decisions relating to data processing and, where appropriate, undertaking privacy impact assessments.

## CHANGES

**Lawfulness, fairness and transparency** - personal data must be processed lawfully, fairly and *in a transparent manner in relation to the data subject*.

**Limitation** – personal data must be collected for specified, explicit and legitimate purposes. It must not be processed in a way incompatible with those purposes. Further processing of the personal data for archiving purposes in the public interest or scientific and historical research purposes or statistical purposes should not be considered if it is incompatible with the original processing purposes.

**Data minimisation** - personal data must be adequate, relevant and limited to information which is necessary in relation to the purposes for which it is processed.

**Accuracy** - personal data must be accurate and, where necessary, kept up to date. Personal data which is inaccurate having regard to the purpose for which it was processed should be erased or rectified without delay.

**Storage limitation** - personal data must be kept *in a form which permits identification of data subjects* for no longer than necessary for the purpose for which the data is processed. Personal data may be stored for longer periods if the personal data is processed solely for archiving purposes in the public interest or scientific and historical research processes or statistical purposes. Personal data should be stored subject to the implementation of appropriate technical and organisational measures to protect the data.

**Integrity and confidentiality** - personal data must be processed in a manner which ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, *using appropriate technical or organisational measures.*

**Accountability** - the controller shall be responsible for and be able to demonstrate compliance with these principles.

## Actions

The grounds for lawful processing broadly replicate those in the Data Protection Act.
However:

- ensure you are clear about what the grounds for lawful processing relied on by your organisation are
- check these grounds are applicable under the GDPR
- review where you rely on consent in an employment context, and consider whether other grounds can be used instead (particularly legitimate interests)
- ensure your internal procedures enable you to demonstrate how decisions to use data for processing purposes have been reached and that all relevant factors have been considered.

## COMMON GROUNDS TO PROCESS DATA LAWFULLY WITHIN AN EMPLOYMENT RELATIONSHIP

### Legitimate interests

Legitimate interests can be a lawful basis for processing for private sector employers, and will be the most common lawful ground to process data in an employment context. The processing is only lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". Recent case law clarifies that organisations cannot simply argue that they have satisfied the 'legitimate interests' test because it is in their economic interests to process the data. However, commercial benefit can be sufficient to count as legitimate unless it is outweighed by harm to the individual's rights and interests. Part of ensuring this balance will involve being "fair, transparent and accountable". So, for example, there may be a legitimate interest in monitoring employees but, in order to help ensure that the employer's interests are not outweighed by the rights of the employees, there must be full transparency about what monitoring takes place and for what purposes, and appropriate safeguards. If, therefore, you rely on legitimate interests, you will need to balance the pursuit of your interests against the rights of data subjects. Make a record so you can demonstrate your assessment of the rights and freedom of data subjects balanced against your business' own legitimate interests.

Be aware that data processed on the grounds of legitimate interests can be subject to a right to object to processing which can only be rejected for "compelling" reasons.

The main legitimate interest for employers will be the storing and transmission of personal data within a company or group of companies for administrative purposes, such as making salary payments, and to ensure that the terms of the employment contract are being performed. If the administrative requirements are international, note that there are additional requirements for transfers of international data. Additional legitimate interests include data processing for the purposes of ensuring network information security, and reporting possible criminal acts or threats to public security to a competent authority (for example in respect of tax or immigration compliance).

Public authorities cannot rely on legitimate interests to legitimise data processing carried out in the discharge of their public functions. There is an on-going debate about organisations such as universities which have some public and some private functions but the draft Bill makes it clear that if an organisation is considered a public authority for the purposes of the Freedom of Information legislation, it will be a public authority under the UK Bill.

### Necessary for performance of a contract or to comply with a legal obligation

Processing is also lawful where it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the data subject's request prior to entering into a contract (which includes employment contracts), and where it is necessary in order to comply with a legal obligation.

### Tax and immigration records

There are specific exemptions for processing information in respect of paying tax, and under the Bill a new exemption has been added to cover data processed for the maintenance of effective immigration control and investigation, and detection of activities which would undermine effective immigration control.

## Actions

Ensure you have considered what grounds for lawful processing will be relied on by your organisation.

If you are a public authority and up until now relied on legitimate interests for processing personal data, identify another basis on which to process the data (typically where processing is necessary in the public interest or in the exercise of official authority).

If you are relying on legitimate interests, ensure that you can demonstrate the balancing exercise between the interests of a controller (or third party) and the rights of data subjects. Consider whether the data subjects would reasonably expect their data to be processed on the basis of the legitimate interests of the controller or third party.

If you rely on legitimate interests, ensure this fact is included in the information provided to the data subject, for example in a data protection policy or privacy notice.

If you rely on legitimate interests in respect of processing, this needs to be set out in an information notice. Employers need to decide whether they are going to use consent (which is not recommended) or legitimate interests in respect of processing employee data.

### Consent

Consent remains a legitimate ground to process data, but is subject to additional requirements. These include limitations on "bundled consent" or offering of services contingent on consent.

Consent cannot be relied on if there is an imbalance in power between the parties. There is inherently an imbalance of power in the employer/employee relationship and therefore consent given in an employment context is likely not to be valid.

***We do not recommend that consent is used as the basis for processing employee data apart from in limited circumstances such as to reply to requests for information from banks when employees are making mortgage applications****. If nonetheless you wish to use consent in order to process employee data this must now be set out in a separate document, which is not part of an oral or written agreement (for example an employment contract) and must be both clearly presented, and easy to revoke.*

It is important to be clear about the grounds for lawful processing and whether or not consent is additional to, or instead of, processing on another ground.

If you choose to rely on consent for processing HR records, **you need to check that**:

- consent is current and active. It should not be consent by inaction. It should not be consent by inactivity, and not by a pre-ticked box
- consent is distinguishable, clear and not bundled with other written agreements and declarations. As such, a separate data protection consent needs to be given to all employees and not included within their employment contract. It must be a separate document akin to a working time opt-out.

Data subjects who provide consent must be informed they have the right to withdraw their consent at any time, but that this will not affect the lawfulness of processes based on consent before its withdrawal. It will also not prevent the employer from processing data based upon the company's legitimate interests but you must ensure you are clear about those interests. It is not recommended that you seek consent in circumstances where you intend to rely on other grounds for processing in any event: this can be seen as misleading and inherently unfair.

A simple method for withdrawing consent needs to be provided including methods using the same medium as that used to obtain the consent in the first place.

## SPECIAL CATEGORIES OF PERSONAL DATA (SENSITIVE PERSONAL DATA)

Where the processing relates to sensitive data, it is more important to be sure you are clear about the grounds relied on to process the data and check the grounds are still applicable under the GDPR. You will need to have an **appropriate policy document** (probably your data protection policy) setting out how you will deal with the data.

### Information notices

You must provide information notices to your staff and candidates to ensure transparency of processing. This should include information in respect of retention periods. The information notice should be clear and concise.

## SUBJECT ACCESS

Under the GDPR, as under the current Data Protection Act, individuals (including employees) may request details of the information which the data controller holds in relation to them. Subject access requests (SARs) are often used as a negotiating chip or aggravating feature when employers and employees are in dispute. However, they must be complied with: failure to comply can lead to significant fines.

Under the GDPR, the data controller (employer) will normally have one month to respond to the request, as opposed to the current 40 days. If a request is particularly onerous, there can be a two-month extension, and in some cases a fee may be charged (this will be unusual and the detail of this aspect of the SAR regime remains to be clarified).

Employers need to:

- be able to identify when a SAR is made
- know who will deal with it
- be able to respond within a month
- have a general protocol for responding to a SAR
- put a specific game plan in place for responding to each individual request.

Being able to demonstrate how you have responded to a SAR, what protocols you have used, what training is given to those responding and how decisions about information disclosure have been made are key to demonstrating compliance.

### Employee monitoring

In light of the growth of homeworking, remote working and "bring your own device" policies, there has been blurring of the lines between work and home. This raises the risk that individuals are increasingly monitored in a private context. Employers may have a legitimate interest in monitoring in order to improve efficiency and protect the company. However, workplace monitoring cannot be intrusive and, if it is, it will be unjustifiable. Monitoring must be transparent.

Employee monitoring must therefore be a proportionate response to the risk which an employer faces. Employers should therefore consider:

- the activity that they are proposing to monitor
- the method of the proposed processing of the personal data, to ensure it is fair to employees
- whether the processing of the activity is proportionate to the concerns raised
- whether the processing activity is transparent
- the nature of the concerns which the employer seeks to abate.

### Legal grounds for employee monitoring / legitimate interests

Consent will not be a legitimate basis for employee monitoring unless employees can genuinely refuse without adverse consequences. Inaction, such as not changing default settings, is not consent.

Employers may therefore be left with invoking "legitimate interest". The purposes of the processing must be legitimate and the method and technology must be necessary, proportionate and implemented in the least intrusive way. Legitimate interests do not override the fundamental rights and freedoms of employees and therefore a proportionality test is necessary. This can form part of the data privacy impact assessment if one is undertaken.

Mitigating measures should be put in place to balance the interests of the employer and the employee's rights and freedoms. Limitations that should be considered may be:

- geographical – where is the monitoring to take place (is it limited to specific places)?
- data orientated – excluding personal files and communications
- time-related
- transparency-related

Employees must be informed of:

- the existence of monitoring
- the purposes for which data is processed and any other information necessary to guarantee fair processing.

New technologies mean the need for transparency is critical and ideally employees should be involved in commenting on the monitoring policies.

In extreme cases (for example where it is suspected that confidential information is being leaked) employers may wish to monitor an employee covertly. There will need to be a careful impact assessment before this is done, and employers should ensure that the level and scope of the monitoring is appropriate and lawful: for example, private email addresses should not be accessed.

### Automated decisions

Data subjects have the right not to be subjected to decisions made by the automated processing of data. This covers matters such as performance at work. If automated decision-making is necessary, it can be used, but it is not without difficulties and should be avoided if possible. This does not stop the use of automated information where the decision is made by the employer and not automatically by the system itself.

### Devices

When connecting personal devices, data protection by design and default means that the devices should be the most privacy-friendly.

## DATA PRIVACY IMPACT ASSESSMENTS

Data monitoring is a specific business risk, and impact assessments should be undertaken.

### Social media

Employers cannot assume that they are entitled to inspect social media during recruitment even if it is publicly available. A legal basis is still required such as legitimate interest, and the employer will need to take into account whether the profile is related to business or private purposes.

Even if social media is inspected, only data which is necessary and relevant to the job may be collected and the data should be deleted as soon as it becomes clear that an offer of employment will either not be made or not accepted. Individuals must be notified of the processing in advance.

Once an individual is an employee, screening of social media should not be taking place on a general basis.

There can be exceptions: for example, if social media monitoring or LinkedIn profiles or similar help provide information in respect of the enforcement of restrictive covenants, because that would be monitoring for the protection of the employer's legitimate interests. It may also be permissible to monitor social media on a limited basis if there is a real risk of bringing an employer into disrepute. However any exception will need to be considered on a case by case basis.

### Monitoring ICT

If an employer uses inspection appliances to decrypt and inspect traffic and record or analyse an employee's online activity, then monitoring may be possible. Cloud based applications may also involve processing of private material such as appointments on a calendar. Although there may be legitimate interests in protecting networks, monitoring all online activity is disproportionate. Less invasive methods should therefore be investigated.

Technology needs to be correctly configured taking into account privacy settings. Employees must be notified of the types of monitoring that take place.

### Monitoring outside the workplace

It is necessary to balance the risks posed by home and remote working in a proportionate manner. Mobile device management enables employers to locate the devices remotely. Data privacy impact assessments should therefore be carried out prior to the use of any such technology and employees must be informed of tracking that is taking place and consequences for it.

### Vehicle monitoring

Employers may have legitimate interests in tracking vehicles. However employees should be given the option to turn off tracking during personal use. Employees should be informed if tracking devices are going to be used.

### Sampling instead of continuing monitoring

What employers should be doing now:

- Consider why they wish to monitor employee activity. What is the legitimate business interest?
- Remember that just because the technology "can" do something that does not mean it must be used.
- Undertake an impact assessment.
- Notify employees of the monitoring policies.
- Consider whether random sampling of activity is appropriate or helpful.

The message is that monitoring of employees *may* be acceptable and *may* be lawful, but care should be taken to assess why the monitoring needs to be done, and ensure that it is not excessive. It may be that instead of constant monitoring, "random sampling" can be done to check employee compliance with business-critical arrangements.

## Actions

### Updating the HR process to be GDPR compliant

As many if not all standard form employment documents will involve processing data, there is a window between now and May to ensure that data processed throughout the employment relationship continues to be processed fairly and lawfully, and that the HR processes are compliant with both the GDPR and the Bill.

We therefore recommend that you:

1. Review standard HR documentation at all stages of the employment process including applications/recruitment, offer letters, contracts, handbooks, and general data handling policies.
2. Work with the rest of your organisation to develop privacy notices for HR processes.
3. Work with the rest of your organisation to consider and update your document retention policy.
4. Draft an appropriate policy document to explain how you comply with the principles in the GDPR and how your retention and erasure policies work.
5. Review any employee monitoring processes and undertake impact assessments if employee monitoring will continue

## FIND OUT MORE

**For further information, please contact:**

**HILARY ALDRED**
**T: +44 (0)1223 465465**
**E: hilary.aldred@penningtons.co.uk**

**DAFF RICHARDSON**
**T: +44 (0)1865 813647**
**E: daff.richardson@penningtons.co.uk**