The rise of the intelligent business: Spotlight on employers

This briefing is the second in our multi-disciplinary GDPR series which aims to help you successfully navigate the GDPR as 25 May 2018 approaches. Here we place the spotlight on key compliance considerations in the employment sphere.

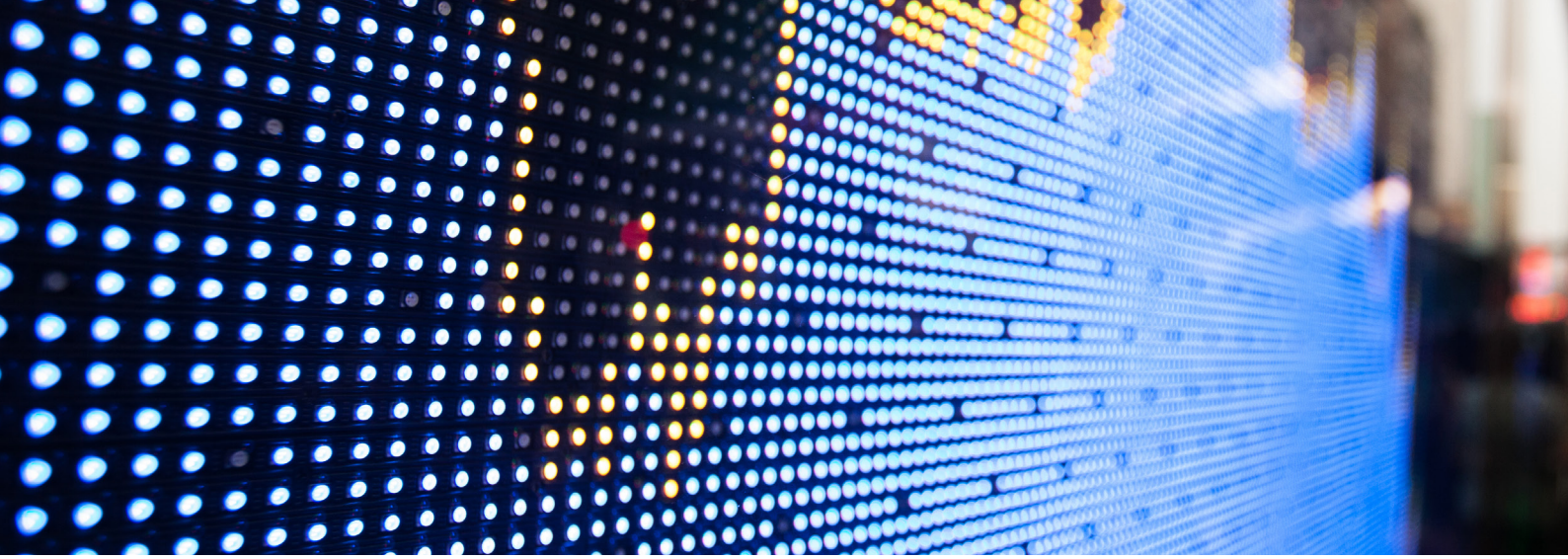
Please click **here** to subscribe to our 'Practical GDPR series'.

Data is ubiquitous in the employment context: it is processed from the point at which a job application or CV is received if not before (such as profiling of potential candidates through LinkedIn, for example), right through to beyond the termination of employment (for example when references are given). The employer will handle "core" categories of employee data on an employee's personnel file (for example, their address, national insurance number, performance appraisals, grievance and disciplinary records), but also data generated and processed in the context of pension schemes and share plans, as well as in liaising with third party providers such as insurers, payroll providers and occupational health professionals. It is worth noting that whilst we refer to "employees" in this briefing, the contents apply equally to employees, workers and self-employed contractors.

In particular, we consider some of the key requirements of the GDPR in the employment context, together with practical tips on how to implement the required changes.

Please click on the links below for more on the following issues:

- Identifying a legal basis for processing employee data;
- Employee rights under the GDPR;
- How to transition to the new regime;
- Sensitive personal data;
- Monitoring and profiling; and
- Training and awareness.



Identifying a legal basis for processing employee personal data

Firstly, what is the employer's legal basis for processing their employees' personal data under the GDPR?

Consent under the GDPR (Art 6(1)(a))

To date, most employers have relied on employee consent as providing the lawful basis for processing employee data. Consent was sought through a provision in an employment contract, or by implication, such as deemed consent in relation to a bonus or employee share scheme.

Employers now need to reconsider this approach as the GDPR sets a high standard for consent. Consent under the GDPR can only be given if that consent is *"freely given, specific, informed and unambiguous"*. Consent must be very clear and specific. Any form of "deemed consent" will no longer be effective. Further, it must be easy for people to withdraw consent, and data subjects have the right to be told how to do so.

The Article 29 Working Party (**"WP"**) guidance on data processing in the workplace has reiterated doubts that existed as to whether employees can validly give such consent to their employer. This is not a new consideration as there has been debate across Europe about whether employees can give consent for some time. Certainly consent cannot be a precondition of employment. Further, consent will not be regarded as "freely given" where the data subject has no genuine or free choice, or would be unable to refuse consent without detriment. Also, consent would not provide a valid legal basis for processing under the GDPR where there is a clear imbalance in the positions between the data controller and the data subject.

Alternatives to consent

We set out below the three legal bases that are likely to be relevant to employers and consider the following issues:

- Which of the alternative bases can be relied on for which activity?
- What are the implications of relying on these alternative grounds?
- How to reflect this in employment contracts and policies, and communicate it to employees?

1. Necessary for performance of the contract (Art 6(1) (b))

Unlimited processing of employee personal data will not be justified merely by reason of the employee having entered into an employment contract. But data processing that is necessary for the performance of the contract is justified, for example, processing bank account details in order to pay an employee.

Ensure that a different legal basis can be relied on for processing that is ancillary to obligations under the employment contract. The monitoring of an employee's website usage, for example, is very unlikely to be necessary for performance of their employment contract (but may, for example, be justified as being necessary for the purpose of the legitimate interest of the employer to protect their confidential information).

Employee share plan awards and other "unilateral" contracts

A question arises as to whether a contract made unilaterally in favour of an employee (such as by deed under English law) could trigger reliance on this ground of processing – an example would be under employee share plans where, commonly, an employee is granted an option or award unilaterally and without signing to confirm acceptance.

In our view, the better approach is not to rely on the "performance of a contract" ground of processing in this case – it is not clear that to do so would be in line with a purposive reading of the GDPR – and so an alternative basis should be relied on instead.

2. Necessary for compliance with a legal obligation (Art 6(1)(c))

Processing may be justified where it is necessary for compliance with a legal obligation, for example where the data controller's processing is to comply with tax legislation or pensions auto-enrolment. Again, however, care is required, particularly in a group context, as this requirement relates to a legal obligation to which the data controller is subject, and so would not cover processing required for compliance with a legal obligation applicable to a third-party (such as, for example, an administrator or service provider to whom the employer provides the data).

3. Necessary for the purposes of a legitimate interest of the data controller or a third party (Art 6(1)(f))

Some degree of processing of employees' personal data is likely to be necessary for the purposes of an employer's legitimate interest in pursuing their business by employing (and rewarding) employees. This is not an unlimited right to process data, however. Employers should undertake a balancing exercise to ensure that the legitimate interests relied on are not overridden by the interests or fundamental rights and freedoms of their employees.

An employer's legitimate interest in undertaking many common types of processing of employee data, such as for internal administrative purposes, may often override an employee's interest in protecting their personal data.

However, reliance on this legal basis will require careful consideration where data is being processed in less obvious ways, or where the data processing is more intrusive and potentially impacts an employee's right to privacy. For example, where GPS is being used to track company car usage for work-related insurance purposes, this may go beyond processing necessary for a legitimate interest if the tracking is used during non-working hours when the car is used for legitimate personal use. In any event employees should be made aware of such processing.

Where legitimate interest is relied on as the basis for processing, the data subject has the right to object in certain circumstances. Employers will need to include details of this right in the information provided to employees, usually via a privacy notice or policy. If the employee objects, the employer must stop processing unless they can show compelling legitimate grounds which override the interests, rights and freedoms of the employee or that the processing is for the establishment, exercise or defence of legal claims.

Employee rights under the GDPR

The GDPR also codifies a wide range of rights for data subjects; employers need to consider how they will comply with these in respect of their employees.

Right to be informed

Employee rights under the GDPR include the right to information on (among other things):

- the categories of personal data that are being processed and the purposes of that processing;
- the identity and contact details of the data controller and Data Protection Officer (**"DPO"**) (if an organisation decides it is necessary to appoint one under the GDPR or voluntarily appoints one);
- the legal basis for the processing – including details of the legitimate interest where that ground is relied on;
- the envisaged data retention period during which the personal data will be stored (or, where this is not possible, the criteria to be used to determine this period);
- the recipients, or categories of recipients, with whom the personal data may be shared, and, where applicable, the fact that the data may be transferred outside of the EEA;
- the existence of automated decision-making, including profiling; and
- the right to lodge a complaint with a supervisory authority.

Employees also have the right to:

- access their personal data and rectify their data;
- obtain and reuse their personal data for their own purposes (ie the right to **"data portability"**); and
- have their data erased, have the processing of their data restricted or object to its processing, in each case where certain conditions are met.

Managing data subject rights in action

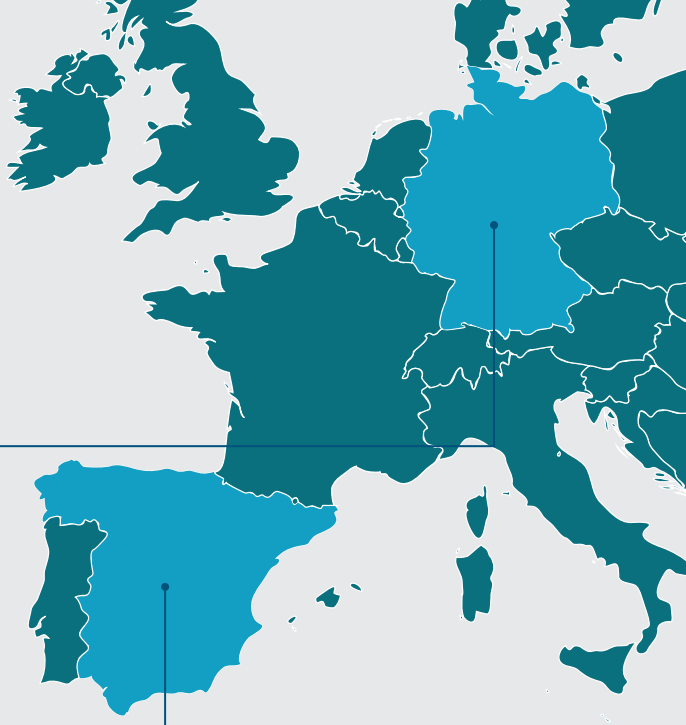
Employers will need to design processes to handle situations where employees exercise their data subject rights under the GDPR. Data subjects can request personal data that a data controller (eg their employer) holds on them (a **"data subject access request"**). This right already exists under the Data Protection Act 1998 (the **"DPA"**) and, in our experience, is being used increasingly frequently in employee-employer disputes. It is important to note that, among other things, the time limit for responding to data subject access requests is shortened under the GDPR so it is crucial that your organisation can handle such requests in an efficient and timely way. In the box overleaf we have set out some of the key changes to the data subject access regime.

With regards to the other data subject rights listed above, the first point for employers to bear in mind is that these are not blanket rights. For example, the right for a data subject to have their data erased is not automatic and only arises in certain circumstances, such as when the personal data is no longer necessary in relation to the purpose for which it was originally collected and when the individual withdraws consent.

Finally, it is worth noting that, for those organisations that need to appoint a Data Protection Officer (**"DPO"**), the GDPR states that a DPO shall not be dismissed or penalised by the employer for performing his tasks. This provides a DPO employee with whistleblowing type protection to seek to ensure they do not feel their employment would be at risk for raising concerns about data protection.

Below we have set out some of the key changes to the data subject access regime:

	Current position	GDPR position
Fee	Can charge up to £10	Must provide for free. Can charge a reasonable fee for additional copies or if an unfounded or excessive request
Format	Any format	If request made electronically, must provide in a commonly used electronic form (unless subject requests otherwise). Recommended to provide the subject with remote access to a self-service system to access their information
Timing	Promptly and within 40 days	Must respond without delay and within one month of receipt. Response can be extended by two months where necessary, taking into account the complexity and the number of requests, by informing the subject of this and the reason for the delay within one month of receipt of the request
Information to be given to data subject	1. Purposes of processing 2. Recipients to whom it was been disclosed 3. Information on the source of the data	Plus: 1. the period data will be stored for 2. the right to request rectification or erasure of restriction of processing, or to object 3. the right to complain to the ICO 4. if automated decision-making used, the logic involved and the consequences of processing 5. if data transferred overseas, information on what appropriate safeguards in place relating to the transfer
Refusal	No need to comply if similar or identical to a previous request unless a reasonable period has elapsed	If request is unfounded or excessive, the data controller may: 1. charge a reasonable fee 2. refuse to act on the request Must inform the data subject without delay (and no later than one month after the request) if not taking action
Remedy and penalties	1. ICO requirement to provide information or impose a fine (up to £500k) 2. Court order for compliance with the subject access request 3. Court claim for compensation for damage suffered as a result of a DPA breach	1. Complain to the ICO, with higher potential fines (up to EUR20mm or 4% worldwide turnover, whichever is higher) 2. Court order for compliance with the data subject access request 3. Court claim for compensation for damage suffered as a result of a GDPR breach



Processing employee data

In Germany

Under the German Federal Data Protection Amendment Act (the **"DP Amendment Act"**), the processing of employee personal data will be permitted in a wider number of circumstances than is permitted under the GDPR. The DP Amendment Act preserves most of the previous provisions on employee data in the current version of the German Federal Data Protection Act.
For example, the personal data of employees may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations in relation to employee representation, collective agreements or other agreements between the employer and employees' representatives. Further, the DP Amendment Act stipulates that personal data of employees can under certain circumstances be processed on the basis of consent. It is deemed that consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests.

In Spain

The Organic Law 15/1999 on Data Protection will be amended to comply with the GDPR. In particular, this will result in the updating of the existing legislation to include:

- The obligation for consent to be freely given, specific, informed and unambiguous;
- The requirement to appoint a DPO in certain circumstances;
- The requirement to carry out impact assessments before processing sensitive personal data;
- The introduction of the 'right to be forgotten'; and
- The obligation to report data breaches to regulatory authorities.

How to transition to the new regime

Employers must devise a practical method for providing employees (as data subjects) with certain information about how their personal data will be processed. The Information Commissioner's Official Guide to the GDPR provides that information must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language; and
- free of charge.

A privacy policy can be drafted to provide all the necessary information and made available to staff, for example in an Employee Handbook or on the staff intranet. Ensure that the policy is available to all employees, including those who do not have access to your organisation's intranet page and it is drawn to their attention.

Preparing a privacy policy requires the employer to consider:

- its legal grounds for processing employee personal data (see above) – there may be different grounds for different aspects of processing; and
- its policy on data retention ie how long employee personal data is stored for.

Employers may have legitimate business reasons or legal obligations to retain data, such as to comply with HMRC requirements albeit the retention periods may differ. However, a fine balance must be struck between an employer's legitimate business interests and their employees' rights. Employers should consider whether to "thin the file" of data that they hold on an employee once they leave the organisation to ensure they retain only what is strictly necessary. Employers should document the thought-process behind any data retention periods; there is a renewed emphasis on record-keeping in the GDPR.

The privacy policy can be amended over time to be kept up-to-date without needing to amend employment contracts. Employers should make clear that the policy is non-contractual.

What should an employer do if their employees gave consent to the processing of their personal data, for example through their current employment contract, prior to the GDPR coming into force?

We recommend writing to employees to inform them of your organisation's updated privacy policy (which will set out the legal bases for processing their data), providing them with a copy of the policy or a link to where it can be found, and using the opportunity to remind them of their reciprocal obligations to inform their employer of any changes to their personal data (eg a new address) and to handle other people's data with care. This assumes the employer is not relying on consent.

The privacy policy is likely to be the focal point of the GDPR compliance programme in respect of employee personal data, but don't forget to review and update other related policies, such as IT access and monitoring policies, as well as employment contracts and other agreements.

Approach to GDPR compliance in employee pension plan and employee share plan documentation

As well as processing data for their core employment practices, employers may also find that they are processing data for specific purposes, where particular considerations arise, such as for pension plans, employee share plans or other benefit and incentive arrangements.

In these cases certain aspects of the GDPR analysis may differ: for example, the purposes for the data processing may differ from the purposes in respect of core activities, and also particular data transfers may need to be catered for. For example, trustees and administrators, to whom data transfers may be made, will be subject to their own GDPR obligations, and they may need to discuss these with the employer to ensure their own compliance. Employers should engage with these requests for information/discussions. Trustees and administrators may also need to send their own privacy statements to employees.

Specific additional information such as relevant national derogations may need to be provided to employees, and employers will need to consider how to document this. However, employees could then be referred back to the main privacy policy where the bulk of the required information would be provided. Indeed, this approach may be preferable, as providing the common information to employees in a single document not only avoids unnecessary repetition but may reduce the risk of inconsistencies or omissions.

Sensitive personal data

Particular care is needed when handling special categories of employees' personal data (formerly known as "sensitive personal data"), such as data identifying racial or ethnic origin, sexual orientation or data concerning health.

The GDPR provides a general prohibition which states that the processing of all special categories of personal data is prohibited without the explicit consent of the data subject (Article 9(2)(a)), but there are a number of exemptions.

There is an exemption if the processing is *"necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment ... law"* (Article 9(2)(b)). This could apply, for example, when an employer needs to ascertain what reasonable adjustments need to be made for a disabled employee.

An employer can rely on this exemption if it has an "appropriate" policy document in place (ie one which explains the employer's procedures for securing compliance with the key data processing principles in respect of the health data and also explains the retention and erasure policy in respect of such health data).

There is also an exemption in Article 9(2)(h) which allows for the processing of special categories of personal data if it is necessary for the assessment of the working capacity of the employee. This processing can only be done under the responsibility of a medical professional subject to the obligation of professional secrecy (eg a doctor).

There is no special exemption for equal opportunities monitoring (and the processing of, for example, racial, gender, ethnic origin or sexual orientation data) in the GDPR. But there is an exemption in Schedule 1, Part 2, paragraph 7 of the draft Data Protection Bill (as at December 2017) which allows an employer to process "specified" categories of data (ie race, ethnicity, religious and philosophical beliefs, health and sexual orientation data, although interestingly not gender) if it is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment. There are conditions for relying on this exemption including that the processing must not be carried out for the purposes of making a decision in relation to a particular individual and there must be an "appropriate" policy document in place (see above).

Criminal convictions

Neither the GDPR nor the Data Protection Bill classify criminal convictions as "special categories of data". This is surprising. However, there is a separate provision in Article 10 of the GDPR which contains a general prohibition against processing personal data relating to criminal convictions and offences, including allegations of an offence. The Data Protection Bill states that data relating to criminal conviction data can be

processed if it is necessary for the purposes of performing or exercising obligations or rights of the employer under "employment law". This suggests that employers can carry out criminal records checks where employees must be subject to the enhanced DBS regime (eg for roles working with children or vulnerable adults or certain roles in financial services).

In relation to normal pre-recruitment criminal record checks (ie in circumstances where the employer is not legally obliged to carry out criminal record checks) it seems that the only option available to employers would be express consent. However, given the difficulties with an employee being able to "freely" consent (and the fact that an employee can withdraw consent at any time), the current state of play suggests that normal pre-recruitment criminal record checks are prohibited without that consent. However, it should be noted that the Data Protection Bill is currently only in draft form so it may be that this issue is clarified either in the final legislation or by way of guidance from the Information Commissioner's Office.

Monitoring and profiling

Under the GDPR, employees will have rights to greater transparency in relation to how they are monitored. Employers should amend their privacy and IT Acceptable Use policies to reflect this. These policies must be accessible to all employees and transparent about any employee monitoring taking place. If an employer wants to use employee data for a purpose that is different to what the data was collected for, this needs to be clearly explained to the employee. In addition, employees should be informed of their right to object to this monitoring in certain circumstances.

The importance of clarity and transparency with regards to employee monitoring was highlighted in the recent case of *Barbulescu v Romania*. This decision held that employees have a reasonable expectation of privacy in the workplace. Where an employer wishes to monitor emails and messages, it must tell the employee that their communications might be monitored. In Barbulescu, although the employee knew it was forbidden to use work computers for personal purposes, he had not been told that his employer was monitoring his communications. As a result, his employer had breached his right to privacy under Article 8 of the European Convention on Human Rights. Following this case employers need to be more transparent about how they undertake monitoring in their monitoring policy.

Profiling is an advanced form of monitoring. It involves (i) the automated processing of personal data; and (ii) using that personal data to evaluate certain personal aspects relating to the individual, in particular to analyse or predict certain aspects concerning their performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movements in a way that has a legal or similarly significant effect on them. The term "automated processing" refers to decisions being made by a computer without human intervention. An example of profiling would be if an employer uses automated decision-making to filter out applicants for a job role based on their personal data, such as their exam grades, without human intervention.

Under the GDPR, not only will employers have to inform candidates about the existence of this automated decision-making, they must also provide "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing*". This will require them to tell candidates how they operate automated decision-making (for example, to filter out those without at least AAB in their A-levels). The automated processing will either need to be necessary for the performance of a contract or the candidate's explicit and informed consent must have been obtained. The candidate should also be given the right to obtain human intervention, to express his or her point of view and to contest the decision.

Training and awareness

Employers must take steps not merely to comply with the requirements of the GDPR, but to be able to actively demonstrate compliance. This represents a departure from the current position under the DPA, which has no equivalent obligation.

More specifically, data controllers and processers are required to implement appropriate technical and organisational measures to ensure, and to be able to provide evidence, that processing is being performed in accordance with the GDPR. In so doing, they must take into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for data subjects' rights and freedoms. These requirements, taken together, underlie the principle of "accountability" – one of the key tenets of the GDPR.

Establishing an appropriate privacy policy (see above) and ensuring that policy is known about and easily available is one way to demonstrate accountability; separate to that is

the need to effectively implement that policy with a view to entrenching the spirit of the organisation's privacy measures into day-to-day operations, across every business unit that processes personal data. The more ingrained employees' awareness of the requirements of the GDPR and how it impacts on their role, the better incorporated the organisation's privacy principles will be within its fabric, and the lower the risk of a breach.

Central to achieving this goal is the delivery of structured employee training on privacy and data protection measures at all levels of the organisation. It is important to remember that successful implementation is an evolving exercise, so employers should ensure that employees receive routine refresher training and that new recruits are adequately briefed and in a timely manner. This will include educating senior management about the requirements of the GDPR and the impact of non-compliance.

From an organisational perspective, non-compliance runs the risk of hefty fines, adverse publicity and reputational damage. Whilst under the GDPR there is no personal liability for staff when a company breaches the legislation, the Data Protection Bill does provide for officers of the company, or shareholders where the affairs of the company are managed by them, to be personally liable where a criminal offence is committed under the Bill *"with the consent or connivance of or attributable to neglect"* of that individual. Offenders will be *"liable to be proceeded against and punished accordingly"*. Note that this personal liability is not a new offence; the wording in the Bill mirrors the current legislation under the Data Protection Act 1998. It is also important to bear in mind that it only applies in the narrow circumstances where a criminal offence is committed under the Data Protection Bill. More concerning for directors will be the Information Commissioner's support for making directors personally liable for breaches of data protection law by their companies, which she expressed during a select committee hearing on the Digital Economy Bill in October 2016. However, that position is not currently reflected in the Data Protection Bill.

Meanwhile, the GDPR places DPOs under a specific obligation to carry out certain tasks. These include to:

- inform and advise a data controller's or processor's employees who carry out processing of their obligations under data protection law; and
- raise awareness and train staff involved in processing operations and related audits.

There is no equivalent explicit training obligation on organisations that are not required to appoint a DPO. However, organisations that fail to establish policies that set out how to comply with the GDPR, in tandem with implementing training to ensure those policies are adequately brought to employees' attention and are properly understood and assimilated, will inevitably struggle to effectively demonstrate compliance.

In addition to rolling out training, it is helpful to record and monitor its delivery and completion, which will form a component of the organisation's reporting obligations.

It is worth noting that the ICO will assess a company's overall commitment to data protection; the delivery of, and quality of, that training will be an essential part of that assessment.

The aim of training sessions should be to raise awareness amongst employees of the generic rationale behind the GDPR, employees' job-specific obligations in handling other employees' and third parties' data, the risks to them personally of failing to comply with their obligations (including disciplinary sanctions up to and including dismissal), and the potentially enormous risks to the organisation of a data breach from both a financial and reputational perspective. These training sessions are also a good opportunity to highlight to employees that if they take the personal data of others (eg clients) without their employer's consent, for example when leaving employment, this could be a criminal offence, liable to prosecution.

The training should be as practical as possible, advising employees what to do in specific scenarios, both to avoid breaching the GDPR in the first place, but also what to do if a breach has occurred.

Examples of areas that training sessions on the GDPR should cover include:

- privacy and confidentiality obligations for those handling data;
- security processes that should be adhered to in order to protect personal data during processing;
- the processes for destroying or returning personal data;
- identifying a data breach;
- responding to data breaches; and
- the potential consequences of failing to adhere to the GDPR.

The most efficient and cost-effective solution is likely to be an e-learning course, particularly for larger organisations. These also have the advantage of becoming a reference tool that can be returned to when employees wish (or are required) to refresh their GDPR knowledge. However, for key staff, larger organisations processing high volumes of personal data or monitoring data on a large scale, or smaller organisations, face-to-face training with scope for role-specific case studies to be discussed and questions to be answered may be a more effective delivery method.

What should employers do to keep employees' data protection knowledge up to date?

Privacy policies must obviously be kept up to date to ensure they are aligned with any changes in applicable legislation, precedent and processing activities. Employers may want to consider appropriate mechanisms for drawing these updates to employees' attention, perhaps by emailing the updated policy to staff when any key changes have been made and asking them to confirm that they have read and understood the updates. Reminders of data protection requirements should also be sent to employees to ensure they remain at the forefront of employees' minds on a day-to-day basis.

The remainder of this **"Practical GDPR series"** will continue to help you deep dive into the detail around the GDPR's key requirements. We are also very happy to discuss GPDR implementation directly with you. We are working with clients on implementation projects right now.

Authors

Christine Young
T +44 20 7466 2845
christine.young@hsf.com

Bradley Richardson
T +44 20 7466 7483
bradley.richardson@hsf.com

Alison Brown
T +44 20 7466 2427
alison.brown@hsf.com

Cat Rawsthorne
T +44 20 7466 2864
cat.rawsthorne@hsf.com