

10 steps towards compliance

Gaela Bailey and Jonathan Fitzgibbons outline the key steps to understanding privacy laws and protecting employee data

Almost all the major markets of the world, with the notable exception of the US, have now implemented privacy legislation to regulate the collection, storage and use of information held about employees by organisations.

Additionally, recent regulatory activity in Europe, new laws in Japan, and high-profile breaches of consumer data security in the US have ensured that data security and privacy laws have become a corporate priority.

At first glance, achieving compliance with these laws can seem a complex, onerous and expensive project. And for HR professionals working as part of a global team, managing employee data stored

on centralised employee databases, such as SAP and PeopleSoft, can seem daunting.

However, most data protection laws share common privacy principles, and create similar obligations for private sector employers with respect to the collection, use, storage and disclosure of employee data.

Here are 10 steps that HR professionals can take to comply with these key privacy principles in respect of employee data.

■ Gaela Bailey and Jonathan Fitzgibbons are data protection and privacy lawyers at Crowell and Moring

Step 1: Analyse the data

Understanding the flow of employee data in your business will help you to establish the steps you must take to comply with privacy laws. It may not be possible to identify every piece of information coming into the business, but knowing the main sources is an invaluable first step in any compliance programme.

Top tip: Review the forms used by your HR department to find out what employee data is collected, what it is used for, and by whom.

Step 2: Review the data collected

It can be tempting for organisations to collect any information that might potentially be useful. However, privacy legislation typically prohibits organisations from collecting any personal information unless the collection is necessary (and not excessive) in relation to one or more legitimate purpose specified by the organisation.

Top tip: Review data collection forms to ensure that each piece of data requested is the minimum necessary for employment purposes. Any additional information requested should be clearly identified as optional.

Step 3: Ensure lawful use of data

Most privacy legislation prohibits employers from collecting data about employees unless it is collected in a manner that is fair and in circumstances that are lawful.

Collection is usually fair if the employer has informed the employee of the purposes for which the data is being collected, and has provided the details set out in Step 4.

Collection will usually be lawful if the employee has consented, or if it is necessary for the employer to comply with legal obligations or obligations arising out of the employment contract.

'Consent' can sometimes be implied. For example, an employer may inform an employee of a proposal to transfer their employment file, unless they object. If the employee doesn't, they can be said to have given 'implied consent' (also called 'opt-out consent'). Whether this is sufficient will depend on the circumstances.

However, many privacy laws deem certain categories of personal data to be sensitive. The circumstances under which such data can be collected are limited.

Top tip: Ensure employee consent is obtained where possible.

Step 4: Provide relevant information

Data protection laws usually require organisations to provide certain information to employees at the time the personal data is collected, or as soon as is possible thereafter. This usually includes telling the employee: the purpose for which the information is being collected; contact details for privacy complaints or queries; the identities of any third parties who may access the data; whether the information will be exported overseas; and whether it is mandatory to supply the information.

Top tip: Draft a standard clause containing this information for insertion into employment contracts, policies and forms used to collect employee data.

Step 5: Manage the storage of data

Data protection laws discourage organisations from retaining personal data for longer than is required for the original purpose for which it was collected, or any other legal requirement. Storing information indefinitely increases the risk of unauthorised access and also means the accuracy of the data erodes. Excess data storage also represents an unnecessary cost to your organisation. Most laws also require the accuracy of the information to be maintained, where relevant.

Top tip: Implement document retention and destruction procedures, specifying how long different types of employee data may be retained. Resist the temptation to specify retention periods that are longer than legally required 'just to be safe'. Periodically purge employee data to ensure that it is accurate and up to date, taking into account any 'hold' orders that may exist due to litigation. Ask employees to inform you if their personal data changes, and clearly mark data as inaccurate where an employee has informed you that this is the case.

Step 6: Implement security measures

Data protection laws require that technical and organisational security measures are used to protect personal data held by organisations. What constitutes technical security depends on currently available technologies, and the amount of cost and effort put into security and maintaining accuracy should reflect the sensitivity of the information and the likely effects of unauthorised disclosure. For most databases, effective password protection and firewall protection is sufficient, and, for most manual files, swipe-card entry or other area restrictions will suffice. Organisational security measures include restricted access to databases and guidance for those with access to employee data.

Top tip: Review existing technical security measures and adopt new measures to ensure the security of employee data, if appropriate. Provide procedural guidance and training to those who handle employee data.

Step 7: Review further use of data

As a general rule, once employee data has been collected by an organisation, privacy laws only permit its use or disclosure for reasons that are compatible with the purpose for which it was originally obtained.

Top tip: Review the uses that are made of employee data once it has been collected by your organisation. Be aware that you may be required to notify and obtain the consent of employees to use their personal data for a purpose unrelated to that for which it was originally collected.

Step 8: Review third-party contracts

Data protection laws usually require employers to ensure that third-party providers of services, such as employee benefit providers, contractually guarantee that they will safeguard employee data.

European data protection laws state that transfers of employee data from the EU to any entity in the US or other non-approved countries may only be made in limited circumstances. These include: where the transfer is necessary in relation to the performance of an employment contract; where the data is protected by a contractual arrangement between the sender and recipient; and where the recipient company has binding corporate rules that ensure the protection of the data.

In the US, organisations can choose to participate in the Safe Harbor scheme run by the Department of Commerce. To participate in the scheme, firms must certify that they will protect personal data in accordance with a list of principles published by the Department of Commerce. Any personal data transferred to a US Safe Harbor company will be deemed to be adequately protected.

Top tip: Review third-party contracts and amend them if necessary to ensure they include appropriate data protection language, including indemnities from third parties for any damages incurred as a result of a breach of data security. Review the situations in which employee data is transferred from the EU to countries such as the US – for example, information stored on an employee database with a server located in the US – and ensure that the legality of each transfer has been considered and addressed.

Step 9: Review employee access to data

Data protection laws provide employees with rights, including a right to access and rectify any inaccurate data held on behalf of their employer.

Top tip: Implement access procedures establishing the scope of accessible data, as well as appropriate formats and timeframes to respond to employee requests.

Step 10: Be aware of local laws

The previous steps outline practical measures that HR professionals can take when handling employee data to assist in achieving compliance with the key principles common to many data protection laws. However, it is important to ensure that legal advice specific to countries and regions is also sought.

Top tip: Seek the advice of legal counsel on the vagaries of applicable local laws, such as national notification requirements, and adjust your business practices accordingly.

'As a general rule, once employee data has been obtained, privacy laws only permit its use for reasons that are compatible with the purpose for which it was originally obtained'