How to determine the legal grounds for processing employee data under the General Data Protection Regulation (GDPR) manager's guide

CONTENTS

INTRODUCTION

The General Data Protection Regulation will apply from 25th May 2018, and employers will need to comply with the GDPR data protection principles when they are processing employees' personal data. For data processing to be lawful, one or more of six legal bases for processing set out in the GDPR must apply.

The employer will need to identify the legal basis for processing in advance to ensure that it is complying with the lawful processing principle and is able to demonstrate its compliance. It will be impossible for the employer to understand the extent of an employee's data subject rights or to draft a compliant privacy notice without first identifying the legal basis for processing.

THE LEGAL GROUNDS FOR PROCESSING

There are six grounds for processing personal data under the GDPR. These are that:

- the data subject has consented to processing for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the data subject's request prior to entering into a contract;
- processing is necessary to comply with a legal obligation of the data controller;
- processing is necessary to protect the data subject's vital interests or those of another person;
- processing is necessary for the performance of a task carried out in the public interest; and
- processing is necessary for the purposes of the data controller's legitimate interests (or those of a third party), unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Consent is unlikely to provide a suitable legal basis for processing most types of employee data.

The three legal bases most relevant in the employment context are performance of a contract, compliance with a legal obligation and legitimate interests of the employer.

Consent

Many employers have relied on consent as a basis for processing employee data. Employers have commonly included data protection consent clauses in employment contracts.

The GDPR makes it clear that consent to processing will be valid only if:

- it is freely given, informed, specific and unambiguous;
- it is obtained by a clear affirmative action;
- where it is obtained in a document containing other matters, it is clearly distinguishable from the other matters, is in an intelligible and easily accessible form, and uses clear and plain language; and
- the employee has the right to withdraw consent to processing at any time, and withdrawing consent is as easy as giving consent in the first place.

The recitals to the GDPR make it clear that consent will not be a valid legal basis for processing if there is a clear imbalance of power between a data subject and the data controller. Consent in those circumstances is unlikely to be freely given. The Information Commissioner's guidance confirms that employment relationships usually involve such an imbalance of power, and that employers should avoid relying on consent as a legal basis for processing employee data.

From a practical point of view, it is inadvisable for an employer to rely on consent as a legal basis for processing, as the employee could withdraw his or her consent at any time.

Performance of a contract

Employers will have to process some employee data to perform their obligations to the individual under the contract of employment. For example, to pay employees, employers have to process personal data such as names, working hours and bank account details. Employers are likely to rely on the performance of a contract as the legal basis for processing in that context. This will also be the legal basis for processing data in relation to employees' contractual benefits, for example recording details of absences to ensure that employees receive their entitlement to occupational sick pay.

Compliance with legal obligations

Employers have a range of legal obligations relating to employees. For example, if an employee goes on maternity leave, she has a right to return to work and may be entitled to statutory maternity pay (SMP). Her employer will need to process information about her pay and about the dates on which she starts and finishes maternity leave to make sure it is paying her the SMP to which she is entitled and allowing her to return to work at the appropriate time.

Employers are likely to rely on complying with a legal obligation as the legal basis for processing data in that context. This may also be the case in relation to keeping records of disciplinary and grievance proceedings; processing data in those circumstances is necessary to enable the employer to comply with, for example, the obligation not to dismiss an employee unfairly. Similarly, employers will have to keep records of employees' hours to ensure compliance with the rules on maximum working hours and the national minimum wage.

The employer's legitimate interests

Employers will have to rely on legitimate interests as the legal basis for processing data in any situation where it is necessary to process data but not in connection with the performance of a contract or compliance with a legal obligation.

For example, employers may want to record when employees enter and leave the workplace for security reasons. If the records allow individual employees' entry and exit times to be identified, this will constitute their personal data. The employer does not need to keep this information to perform its obligations under the employment contract or to comply with a legal obligation. It will have to rely on the processing being necessary for its legitimate interests in maintaining security as the legal basis for processing.

A further example of where an employer could rely on its legitimate interests as the legal basis for processing is where it retains personal data about unsuccessful job applicants for a period in case an applicant makes a complaint about the recruitment process. In this case, it is necessary for the employer to process data for its legitimate interests in defending a potential legal claim.

The employer's legitimate interests would also provide a legal basis for processing personal data in relation to appraisals; this would be necessary for the employers' interests in maintaining performance standards.

Problems with using legitimate interests as a legal basis

One drawback to relying on legitimate interests as the basis for processing is that it involves balancing the interests of the employer with those of the employee. If the employee's interests or rights and freedoms outweigh those of the employer, the employer will not be able to rely on its legitimate interests as the legal basis for processing. The more sensitive or intrusive the processing, the more difficult it will be to show that the legitimate interests basis applies. The employer should weigh the importance of the processing against the possible adverse impact on employees, and assess whether or not there is an alternative, less intrusive, way to achieve its objectives. This will help it to demonstrate that it is appropriate to use its legitimate interests as the basis for processing.

Employees have more extensive rights if the employer is relying on legitimate interests as the basis for processing. The employer must tell the employees, in a privacy notice, what legitimate interests it is pursuing. Employees have a right to object to processing based on legitimate interests. If an employee objects, the employer must show that there are

compelling legitimate grounds for processing the data that override the employee's interests or rights and freedoms. The employee can require the employer to restrict data processing (i.e. stop the processing) until it shows that its legitimate interests outweigh those of the employee. The employee can also require the employer to erase his or her personal data if there are no overriding legitimate grounds for processing it.

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL RECORDS DATA

Special rules apply if an employer is processing "special categories" of data (this is broadly the same as sensitive personal data under the Data Protection Act 1998). The special categories of data are data that relates to an employee's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

If an employer processes special categories of data, it has to show that one of the specific legal grounds for processing such data applies. The grounds for processing special categories of data under the GDPR that are most likely to be relevant in the employment context are that:

- processing is necessary for carrying out obligations and exercising rights in the field of employment law, as authorised by national law;
- processing is necessary for the establishment, exercise or defence of legal claims; and
- the employee has given explicit consent to processing for specified purposes.

Personal data relating to criminal convictions and offences is not included in the "special categories" of data, but is subject to similar additional protection.

The Data Protection Bill will allow an employer to process special categories of data and criminal records data where the processing is necessary for performing obligations or exercising rights under employment law, provided that the employer has an appropriate policy document in place.

To be an appropriate policy document under the Data Protection Bill, the document must explain:

- how the employer complies with the GDPR data protection principles in relation to the processing of special categories of data and criminal records data; and
- the employer's policies in connection with the retention and erasure of special categories of data and criminal records data, including an indication of for how long such data will be kept.

The employer must retain, review and update the document from time to time, and make it available to the Information Commissioner on request.

Similar issues arise in relation to relying on consent for processing special categories of data as in relation to other personal data. An employer can rely on employees' consent only if there would be no adverse effects should they choose not to give it or to withdraw it. For example, if an employer runs a voluntary fitness programme for employees as part of a wellbeing strategy, it could ask employees for their consent to process health data that is gathered under the programme. Provided that the programme is entirely voluntary, and there are no negative consequences for employees if they refuse to consent, the employer could rely on consent for processing the data.

The Data Protection Bill includes a limited provision that allows data relating to racial or ethnic origin, religious or philosophical beliefs, health or sexual orientation to be processed for equal opportunities monitoring purposes. This is strictly limited to the types of data mentioned and is subject to certain other limitations, including that the employee can require the employer to stop processing his or her data. The employer can rely on this condition for processing only if it has an appropriate policy document in place.

DETERMINING THE GROUND(S) FOR PROCESSING

A key part of an employer's GDPR compliance programme will be to conduct an HR personal data audit. The audit process involves the employer identifying the HR personal data that the organisation processes and gathering relevant information about each category.

The employer should use the information gathered during the data audit to determine the legal grounds for processing each category of employee personal data. This can be done either as part of the audit process, or as a separate exercise. Essentially the employer should ask itself a series of questions about its reasons for processing data, which will help it decide which legal basis is appropriate in each case.

What is the purpose of the processing? The first question for the employer to ask is why it processes each type of personal data. The employer should record that information as part of the data audit. There may be more than one purpose for processing a particular set of data and the employer should record all relevant purposes. Employers should note that the purpose of processing is different to the legal basis for processing. For example, the purpose of processing data relating to employees' annual leave would include tracking their holiday entitlement and planning absence cover. The employer should go on to identify the legal grounds for processing for each purpose.

Is it necessary for performance of the contract? Once it has recorded the purpose or purposes for processing, in relation to each purpose the employer should ask itself if the processing is necessary for performance of the employment contract. That is likely to be the case where the employer processes relevant data to ensure that an employee receives the pay or other contractual benefits to which he or she is entitled.

Is it necessary for compliance with a legal obligation? The next question is whether or not processing is necessary to enable the employer to comply with its employment law obligations. This is likely to be the case, for example, where it processes data in connection with entitlements to family-related leave and pay.

Is it necessary for the employer's legitimate interests? If the employer cannot rely on the performance of the employment contract or compliance with a legal obligation as a condition for processing, it should consider if the processing is necessary for its legitimate interests. If it is, it should identify and record what those legitimate interests are, consider whether or not its own interests outweigh the rights and freedoms of employees, and record the outcome (using a formal or informal impact assessment as appropriate). The employer may conclude that the impact of the processing on employees outweighs its own legitimate

interests; for example, it could decide that employee monitoring is disproportionately intrusive. Where it reaches such a conclusion, the employer should either stop processing the relevant category of data, or process the data in a way that reduces the impact on employees.

If the processing is not necessary for the performance of a contract or compliance with a legal obligation and the employer is unable to identify a legitimate interest that provides a basis for processing the data, it should stop processing it, except in the limited circumstances in which it may be appropriate to seek the employee's consent.

Recording different grounds for processing

The employer may process the same data for more than one purpose. For example, information about family-related leave is processed to ensure that employees receive their legal entitlements. However, it may also be processed for diversity monitoring reasons, to allow the employer to assess its record on retaining and promoting employees who have taken a period of leave. Processing the data for that reason will be in the employer's legitimate interests and the impact on employees is likely to be low.

Another example of where there is more than one basis for processing is the processing of data relating to disciplinary, grievance or performance issues. This will be necessary to enable the employer to comply with its employment law obligations, but is also necessary to enable it to meet its legitimate interests in maintaining appropriate standards of behaviour and performance within the organisation. Those needs will generally outweigh the rights and freedoms of employees.

If there is more than one basis for processing data, the employer should identify and record all of the relevant legal bases, to ensure that relevant data subject rights are observed. As noted above, an individual has greater rights in relation to data processed for legitimate interests than in relation to data processed for other reasons. Therefore, it is important for employers to record all the reasons why they process a particular type of data at the outset.

Where an employer is processing special categories of personal data or criminal records data, it needs to carry out a similar exercise to identify the legal basis for processing and ensure that one of the relevant conditions for processing applies. This is likely to be particularly relevant to health data, which the employer may need to process to establish an employee's fitness to work and to comply with its obligations to employees with disabilities; to special categories of data processed for equal opportunities monitoring; and to information about an employee's criminal record processed as part of a recruitment process.

As noted above, the employer will need to put in place an appropriate policy on special categories of data and criminal records data.

Next steps

Once the employer has identified the legal basis for processing each category of data, it needs to ensure that this information is included in the privacy notices it provides to job applicants and to employees. If the employer is relying on its legitimate interests as the legal basis for processing, it must identify those interests in the privacy notice.

The GDPR imposes an obligation on organisations to maintain a "record of processing activities", also known as a data register, which must be made available to the regulator (the Information Commissioner in the UK) on request. The register must include information about the purposes of processing. It is advisable for employers also to include the grounds for processing as this will help them to demonstrate that they are complying with the principle of accountability under the GDPR.

Employees may have additional rights associated with certain bases for processing their data. Employers should put processes in place to ensure that they respond appropriately if an employee seeks to exercise those rights, in particular by objecting to processing or asking the employer to delete his or her data.

In the event that an employee objects to processing, the employer should be able to refer back to its assessment of whether or not its legitimate interests outweigh the rights and freedoms of employees. This will allow it to defeat the right to object. Procedures should also be in place to restrict processing of relevant data until the employer's reasons for processing data are verified.

Where an employee requests to have his or her data deleted, the employer should check that the right applies and if there is any other legal basis for continuing to process the data. It can then delete or retain relevant data as required.