GDPR series: Creating and reviewing data protection policies Part 1— Internal-facing policies

In this two part series on creating data protection policies, Ann Bevitt, Partner at Cooley LLP, looks at the changes that will need to be made to internal-facing policies

Many organisations already have a raft of policies and procedures dealing with data protection. These will need to be updated to ensure compliance with the requirements of the EU General Data Protection Regulation 2016/279 ('GDPR'). In addition, companies will be required to create policies to implement new obligations and rights introduced by the GDPR, such as the right to be forgotten and the right to data portability.

Also, given the new principle of accountability introduced by the GDPR, organisations will need such policies to be able to demonstrate their compliance with data protection principles.

This article looks at the changes that will need to be made to internal-facing policies that are made available to employees.

Employee privacy/data handling policy

In addition to providing all employees with privacy notices detailing the processing of their data during their employment, companies should put in place a comprehensive employee privacy (or data handling) policy. This will inform both employers and employees of their data protection responsibilities when handling personal data. In particular, such a policy should make clear to employees why data protection is important, what is meant by 'personal data' and 'processing', and the principles that must be satisfied when handling, disclosing and storing personal data. Employers should make clear that a failure to comply with the policy may result in disciplinary action being taken, up to and including dismissal.

Subject access request policies

Employees, especially those who are in dispute with their employers, often make subject access requests ('SARs') and so many employers already have policies in place dealing with these requests. These will now need to be updated to reflect the GDPR changes. For example, under Article 13(3) of the GDPR, the initial time limit for responding to such a request is reduced from the current 40 days to one month (although there is the possibility of a two-month extension in the case of complex requests). Also, under the GDPR a fee can only be charged if a SAR is 'manifestly unfounded or excessive', e.g. because it is repetitive. Those organisations that routinely levied the statutory £10 fee will therefore have to revise their practices.

It is particularly important that employers handle SARs correctly in future. In its announcement on 7th August 2017 regarding the incorporation of the GDPR into UK law, the government indicated that it intends to create a new criminal offence of altering records with intent to prevent disclosure following a SAR, with a maximum penalty of an unlimited fine.

Policies covering the right to erasure/to be forgotten

In the UK, employees currently have the right to prevent the processing of their data where processing is likely to cause damage or distress to themselves or others, and for direct marketing purposes (see, respectively, sections 10 and 11 of the Data Protection Act 1998 ('DPA'). They also have the right, pursuant to a court order (under section 14(1) of the DPA), to have their inaccurate personal data erased or destroyed.

Under the GDPR, employees' right to erasure of their personal data is significantly extended. For example, as well as being able to prevent the processing of his/her personal data for direct marketing purposes, if an employer relies on consent as the legal basis for processing an employee's personal data, and the employee withdraws his/her consent and there is no other available legal basis, the employee's personal data must be erased.

Also, if the employee objects to the processing of his/her personal data, and there are no overriding legitimate grounds for the processing, those data must be erased.

In addition, if the data are no longer necessary in relation to the purposes for which they were collected, or if they have been unlawfully processed, an employee has the right to have them erased. And an employer's obligations do not stop there: where an employer has made data available to third parties which it is required to erase, it must — taking into account available technology and the cost of implementation — take reasonable steps to inform those now in possession of the data that the employee has requested the erasure of those data.

Although there are some limits to the right to erasure, for example where the processing of the data is in compliance with a legal obligation to which the employer is subject, or for the establishment, exercise or defence of legal claims, it is clear from this brief description of the right that any existing policies covering the right to erasure will need to be substantially amended. Any employers who currently do not have a policy should introduce one so that employees are aware of their right to erasure, as required by Article 12(1) of the GDPR. Additionally and from a practical perspective, whoever is responsible for fulfilling such requests needs to be clear about what is required.

"Although there are some limits to the right to erasure, it is clear that any existing policies covering the right to erasure will need to be substantially amended. Any employers who currently do not have a policy should introduce one so that employees are aware of their right to erasure, as required by Article 12(1) of the GDPR."

Right to portability policies

Article 20 of the GDPR introduces a new right for employees, in certain circumstances, to receive their personal data which they have provided to their employer in a structured, commonly used and machine-readable format which they can then transmit elsewhere (for example, to another employer). This right to portability of data applies where the legal basis for the processing of data is either consent or contract (under Article 20, paragraph 1a) and the employer's processing of those data is automated. The time limit for responding to such a request is one month (although there is the possibility of a two-month extension in the case of complex requests) and a fee can only be charged if a request is 'manifestly unfounded or excessive'. Again, employers will need to create a policy so that employees are aware of their right to portability of their data as required by Article 12(1) of the GDPR, and ensure that those handling such requests are given adequate training.

Right to rectification

Under section 14 of the DPA, employees currently have the right, pursuant to a court order, to have their inaccurate data rectified. Under the GDPR, an employer must rectify inaccurate data 'without undue delay' and without the need for any court order. Rectification can include having incomplete data completed, for example by the employee providing a supplementary statement regarding the data.

As with the other rights already discussed, employers need to make employees aware of this right, and a policy is the obvious way of doing this.

Rights in relation to automated decision-making

Under Article 22(1) of the GDPR, an employee has the right not to be subject to a decision based solely on automated processing, where that decision 'produces legal effects' concerning him/her, or similarly significantly affects them, for example because that decision indirectly discriminates against him/her.

To guard against the risk of such claims, Article 22(4) provides that profiling cannot be based on any of the 'special categories of data' (i.e. data on racial or ethnic origin, political opinions, religions, beliefs, trade union membership, genetic or health status or sexual orientation) unless the individual has explicitly consented, and the purpose of the processing is not prohibited by law, or the processing is necessary for reasons of substantial public interest.

Even if profiling based on such data is permitted, an employer must still comply with the requirements of Recital 71 of the GDPR. That Recital requires an employer to use appropriate mathematical or statistical procedures for profiling, and to implement appropriate technical and organisational measures. Such measures should ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised. They should also secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the individual and that prevent, among other things, discriminatory effects on individuals on the basis of the special categories of data, or that result in measures having such an effect.

Other new rights for employees who are subject to automated decision-making include the right to be notified at the time data are collected not only of the fact that profiling will occur, but also of the 'logic involved' and the 'envisaged consequences of such processing' (Article 13(2)(f)). In addition, where the justification for profiling is either that it is necessary for the entering into or the performance of the employment

(Continued on page 8)

(Continued from page 7)

contract or based on an employee's explicit consent, the employer must implement suitable measures to safeguard an employee's rights and freedoms and legitimate interests. These measures must include the right to obtain human intervention in the decision-making, and the right of the employee to express his/her point of view and to contest the decision. It is unclear what exactly is meant by 'human intervention'. Hopefully this will be addressed by guidance from either the European Data Protection Board and/or Member State data protection authorities, but in the meantime employers should put in place a policy making employees aware of their rights in relation to automated decision-making.

Security incident response policy

Although breach notification is not currently mandatory in most sectors, many organisations already have a security incident response plan. The need for such a plan or policy setting out breach response is increased by the new requirements in the GDPR, namely the mandatory breach notification obligations and the short timeframes for making such notifications (within 72 hours of awareness). Existing policies will need to be updated to reflect these new obligations.

Summary

Whether or not an organisation already has a range of internal-facing policies dealing with data protection, the requirements of the GDPR mean that as part of their GDPR compliance programme, employers need to focus on either revising and/or creating such policies, and rolling them out to employees before May 2018.

Part 2 of this article series, to be published in the next edition of this journal, will address external-facing policies and procedures.

Ann Bevitt
Cooley
abevitt@cooley.com