GDPR in the workplace — 5 key questions to ask

Linda Hynes, Partner, and Declan Groarke, Solicitor, with Lewis Silkin, suggest key questions for employers to consider when reviewing workplace practices

One year on from the frantic scramble to introduce policies, processes and procedures to ensure compliance with the General Data Protection Regulation ('GDPR'), employers are beginning to consider whether those policies and procedures are fit for purpose. We observed how organisations initially focussed on their customer-facing data processing activities, with only limited attention being paid to the processing of employee data. But many employers are now making more concerted efforts to make sure that their workplace policies and practices are meeting their enhanced GDPR obligations. This is no easy task.

In its latest annual report (covering May to December 2018), the Data Protection Commission ('DPC') commented that the complexity of the queries and complaints it received increased post-GDPR, probably because of increased awareness of data protection rights.

In this article, we draw on the trends we've seen over the last year to suggest five key questions for employers to consider when reviewing their workplace practices.

1. Is your privacy notice fit for purpose when it comes to job applicants?

Pre-employment checks can involve a significant amount of processing of personal data, including special category or sensitive personal data. Employers are beginning to recognise that their data privacy notice (which they may have implemented quickly to comply with the GDPR without much bespoke consideration) cannot be a one-size-fits-all solution for both job applicants and employees.

If your privacy notice focuses only on employees, consider whether to broaden its scope to include job applicants or to adopt a specific privacy notice for job applicants. If taking the second approach, the privacy notice for job applicants will still need to integrate GDPR transparency principles, including the purposes for which the data will be processed, but with a marked focus on the pre-employment status of the relationship. For example, the privacy notice may set out separate data retention periods for successful and unsuccessful job applicants. It may explain what further personal data will be processed for job applicants who accept an offer of employment (such as data collected through a medical questionnaire/declaration or equal opportunity monitoring).

Employers should issue the privacy notice to each job applicant on receipt of their application, since they won't have access to the employer's intranet and may not easily find it on the website. This may need to be done through an external recruiter or any recruitment software the employer is using.

2. Do you have a data processing agreement for that recruiter?

Where an employer does use a third-party recruiter, that recruiter will usually just process candidate personal data on behalf of the employer. The employer (as controller) must be satisfied that the recruiter (as processor) has implemented appropriate measures to ensure GDPR compliance and to protect the data protection rights of the candidates (data subjects).

However, the employer should consider if the recruiter is actually also a controller (as well as a processor). For example, the recruiter would be a controller if it intends to send personal data collected from job applicants to other clients. This would mean that both the recruiter and the employer need to have their own privacy notices in place for candidates.

The GDPR requires that any processing carried out by the recruiter as a processer is governed by a contract between the recruiter and the employer known as a Data Protection Agreement, Data Processing Agreement or 'DPA'. The DPA must contain specific provisions about the data processing activities to be carried out by the recruiter; the duties of the recruiter regarding data subject access requests received by the employer; and the duties of the recruiter regarding inspections and audits conducted by the DPC.

The DPC's latest annual report states that there has been a drive to improve data protection compliance through

Linda Hynes is leading a Workshop on 'Data Protection in the Workplace — the Latest Thinking' at the 14th Annual Data Protection Practical Compliance Conference, taking place in Dublin on 14th & 15th November 2019. See www.pdp.ie/conference

investigations and audits. With this in mind, employers and recruiters who may have overlooked these DPA requirements are now ensuring appropriate DPAs are in place.

If there is no DPA, or an imperfect DPA, there may be liability for both the employer and recruiter. However, it is important that you don't simply focus on whether you have a DPA in place with the requisite provisions. The provisions of your DPA need to be implementable in reality. For example, if there is a requirement to delete all personal data at the end of the contract, how will this be evidenced?

3. Does your employee monitoring reflect the new complex realities of work?

Around the world, employers are beginning to use new methods to monitor employees and their devices. For example, biometrics are being used for identification purposes while geolocation and smart devices are being used to monitor the location of employees.

In Ireland, some of these technologies are yet to be introduced, but traditional technologies, such as the monitoring of work emails to ensure employees are not working excessive working hours, are being adapted to help reduce stress and meet health and safety obligations.

The trend in Ireland towards bringing your own device to work is continuing. With the advent of the GDPR and the growing awareness of data protection in Ireland, more and more employers are introducing Bring Your Own Device ('BYOD') policies to monitor how employees connect to and access the workplace network and resources. Employees are used to having their work devices, emails and internet usage monitored, but anything more invasive will likely be questioned. The challenge for employers is trying to figure out how to monitor personal devices used in the workplace (or at home for work purposes) in the same way as they monitor company-owned devices. Flexible working arrangements are adding to this challenge. More and more employees are working from home and as a result, a complex reality exists where employees are working on personal devices and using work devices for personal reasons.

> ***"If there is no DPA, or an imperfect DPA, there may be liability for both the employer and recruiter. However, it is important that you don't simply focus on whether you have a DPA in place with the requisite provisions. The provisions of your DPA need to be implementable in reality."***

Whichever device is used, employers need to ensure that their business is not exposed to risk. Employers are at risk if employees don't know what the business considers to be acceptable usage. The Workplace Relations Commission has been critical of employers who impose sanctions but who do not have an appropriate acceptable usage policy ('AUP') in place or who have failed to communicate it to their employees.

Employees must also be made aware of what monitoring will take place and for what purpose. Obviously, there is a legitimate interest and basic business need for employers to be able to monitor what is happening in this complex reality. However, this must be balanced against the employee's reasonable expectation of privacy. In the absence of a well-communicated policy, it is difficult for employees to assess what level of privacy is afforded to them. Under the GDPR, employees have an expectation of privacy that would be at odds with extensive monitoring and employers must ensure that any monitoring is necessary, reasonable and proportionate. The transparency principle in the GDPR dictates that BYOD and AUP policies, detailing the monitoring of employees and their devices, are clearly communicated to employees. These policies should specify what acceptable use is, what constitutes misconduct and the consequences of improper use both during and outside working hours.

4. Are you getting savvier about DSARs?

Since the implementation of the GDPR, employers have experienced a significant increase in data subject access requests ('DSAR') from prospective, current and past employees. However, employers are quickly becoming sophisticated project managers when it comes to handling them.

Many employers have implemented defined reporting lines for escalation on receipt of a DSAR. Employers are also getting quicker at assessing DSARs. The majority of employee DSARs are general in nature, and without limitation to the data being sought, but employers are becoming savvier at refining their scope. They are more inclined to engage with the employee to refine the request.

A controller has one month to respond to a DSAR, which can be extended by a further two months where the request is complex or the controller has received a number of requests. Employers are taking advantage of this. Before even beginning a search, well-versed employers will seek to limit the scope of a request by seeking more detail about the information the employee is looking for.

Employers who receive large volumes of DSARs are also becoming leaner in how they process and respond to them. Automated software platforms, designed specifically for managing DSARs, are being utilised to process requests which are likely to return a large volume of personal data. These platforms enable multiple persons to review, classify and batch documents simultaneously. They also offer tools to remove

(Continued on page 6)

(Continued from page 5)

duplicates and redact data which should not be disclosed.

An employee DSAR is usually a strong indication that litigation is coming and it's important that employers involve their legal advisors early to manage risks and advise on what should be withheld on the basis of legal privilege or other exemptions.

Finally, employers are shrewdly reviewing their data retention policies. Employers are adopting stricter data retention policies, deleting older data where possible to help reduce the administrative and often cumbersome burden of dealing with DSARs.

5. Do your employees really know what to do about data protection?

There is a growing recognition that if employees do not understand their responsibilities under the GDPR, the employer is set up for failure; and it is the employer who faces penalty, not the employee.

Employees in the IT, Legal and HR departments are not the only ones who need to understand data protection. After all, it is not them who will be accessing and processing personal data to manage operations, communicate with customers or analyse CRM (customer relationship management) systems. Employers need to ensure that all employees are acutely aware of their specific data protection responsibilities and that they actually apply those principles in the day job.

Many employers are now adopting employee 'data protection responsibility' policies. Such policies reiterate the principles of personal data protection, provide rules and guidance on how to handle data and keep data secure and confidential, and explain what to do in the event of a data breach.

Since employees are the main source of personal data breaches, employers should ensure that employees understand:

- what constitutes a data breach, including a serious breach which may need to be notified to the DPC within 72 hours;
- how to react in a breach situation; and
- who to report the breach to (e.g. Compliance Officer or Data Protection Officer) so that person can contain, manage and mitigate risks.

Employees need to be aware that any breach, however small, should be logged. In the event of a DPC audit, squeaky clean data breach logs are not necessarily desirable. An auditor is most interested in the processes for handling data breaches and assessing whether or not they are notifiable to the DPC. Blank data protection breach logs tend to indicate a lack of awareness among employees and call into question how seriously the business takes protection of personal data.

It is not enough for employers to have well drafted policies and procedures in place. Employees have to be trained on the practical implementation of those policies in their day-to-day working lives. We are now seeing many employers rolling out GDPR training which is more bespoke than the general awareness training they rolled out pre-May 2018, and we are expecting to see this trend continue.

Conclusion

Organisations are aware that the maximum fine for non-compliance with GDPR is €20m or 4% of global turnover — more than enough to sink an SME. Although the DPC is unlikely to penalise an employer to this extent, there are other serious consequences of non-compliance that can be difficult to overcome such as harm to goodwill, reputation and consumer and employee trust. Employers are aware of this. The deadline for compliance was 25th May 2018. But, for many organisations, this has turned out to mark the start of the journey, not the end. They are only now getting to grips with the practical realities of GDPR compliance.

Linda Hynes and Declan Groarke
Lewis Silkin
declan.groarke@lewissilkin.com
linda.hynes@lewissilkin.com