GDPR Bitesize
Key Issues for HR

February 2018

Table of Contents

Introduction 3
GDPR HR audit mapping out project success 4
Moving away from consent 6
Getting to grips with Employee Data Privacy Notices 7
Time to update your subject access procedures 9
Data subject rights 10
Effective enforcement and painful penalties: are you up to speed with the new GDPR breach reporting process and enforcement regime? 12
Contact Details 14

Introduction

Welcome to our collection of law-now updates on the HR aspects of GDPR.

We appreciate that when it comes to GDPR compliance, it can seem like an overwhelming task. With that in mind we have broken this topic down into manageable – bitesize – sections, and provided a high-level and practical route map to compliance.

This series highlights the key changes for HR. It does not seek to cover issues like international data transfer, processing contracts or data privacy impact assessments, which will generally be picked up as part of an organisation's wider GDPR planning. These are all areas we and our colleagues can assist with where they are relevant to your HR project.

While the GDPR introduces a new layer of obligations for HR teams, it builds on the existing data protection regime. Businesses should not therefore be starting from scratch, however there are important changes that need to be incorporated into systems, processes and approach.

Perhaps one of the most important changes is the cultural shift that the GDPR is seeking to achieve. In the digital economy that we now live in, the aim is to promote transparency and drive accountability. Employers need to move to a mind-set whereby they acknowledge they are the custodians of the data they hold, and recognise that employees – as data subjects – have a number of new rights reflecting this (going beyond although still including the vital right of subject access).

As we explain in this series, the first step for HR is a data audit – mapping out how your organisation processes personal data, why you do this and where potential compliance gaps might exist. An audit serves many purposes, and one of these is to feed the 'privacy notice' that will have to be issued to all employees and other workers. Many organisations are familiar with these for their customers, but have not issued them to their workforce (or at least not in any detail as will now be required). That approach needs to change.

Your action checklist should also include rethinking the basis of processing, as discussed in our update on moving away from consent, as well as revised subject access procedures and new policies on data protection and retention periods, to name but a few examples!

We can assist with all aspects of compliance, and would be delighted to discuss this with you.

Alison Woods and Melanie Lane

Alison Woods
Partner
T +44 1224 267176
E alison.woods@cms-cmno.com

Melanie Lane
Partner
T +44 20 7067 3653
E melanie.lane@cms-cmno.com

GDPR HR audit mapping out project success

The first step in any GDPR action plan should involve an audit of personal data collected and held by an organisation, to map out how personal data flows through their organisation and systems.

Given the significant volume of personal data held by an HR department, collecting and analysing this data is a time consuming task. There are many forms this could take. Helpfully however, the Information Commissioner's Office (ICO) has now published a template spreadsheet that organisations can use as a starting point in their audit process. Click here to access.

What has changed?

While there have always been record keeping requirements under the Data Protection Act, A.30 of the GDPR contains an enhanced obligation to document processing activities. Additionally, most outputs under any GDPR project will need as their foundation some solid information about the data processing that is undertaken by the department. No use building without foundations!

We therefore recommend that the audit undertaken is done in such a way as to provide a platform on which to build a GDPR action plan.

In HR, the audit will need to encompass the personal data of past, present and prospective members of the workforce and any other individuals who are within the remit of HR's responsibility; this will certainly include employees and job applicants, but is likely to extend to a wider category of individual such as interns, volunteers and self-employed contractors. The audit should encompass personal data that may still be retained in relation to past members of the workforce as this will still be covered by the GDPR regardless of when it was collected.

The audit could be done as a discrete exercise by HR or as part of a wider programme covering:

— not only workforce personal data, but also that of other data subjects such as customers and suppliers; and

— other departments within a business who will also process data e.g. finance, legal and IT.

The audit will serve as a record of the processing activities undertaken by the organisation; this record (which must include certain prescribed details listed below and will need to be kept up to date) must be made available to the ICO upon request. In the UK the record keeping requirement generally applies to organisations employing 250 or more employees, although smaller organisations could also be caught, for example, where the processing they carry out is more than occasional or includes sensitive personal data (known as special categories of data under the GDPR).

Organisations in scope must document the following information:

— The name and contact details of the organisation (and where applicable, of other controllers, and the data protection officer).

— The purposes of processing.

— A description of the categories of individuals and categories of personal data.

— The categories of recipients of personal data.

— Details of transfers to third countries including documenting the transfer mechanism safeguards in place.

— Retention schedules.

— A description of the technical and organisational security measures.

Another factor to consider as part of the audit process are the appropriate retention periods for data, and a plan for secure deletion/destruction of old (beyond justified retention) data.

Under the Data Protection Bill currently proceeding through Parliament, an employer is required to maintain an appropriate policy document explaining how an employer processes special category personal data, which also refers to retention periods and erasure of data. The policy has to be available to the Information Commissioner.

What should your audit cover?

The ICO templates suggests that the audit spreadsheet should consider the following main areas with various sub categories of information.

— Article 30 Record of Processing Activities

— Privacy Notices

— Consent

— Access Requests

— Data Protection Impact Assessments

— Personal Data Breaches

— Data Protection Bill – Special Category or Criminal Conviction and Offence Data

Moving away from consent

A significant issue for HR under GDPR is the justification for processing personal data.

Given the huge volumes of personal data that HR departments deal with, this is a particular concern. Many employers currently seek to address this via a consent clause in their contract of employment, although in reality there are normally other grounds on which the majority of HR processing could be based on. Also, due to the nature of the employee/employer relationship (i.e. the clear imbalance of power) it is unlikely that an employee is able to give their employer valid consent, something that has not been lost on the ICO.

The ICO have also emphasised that seeking consent from an individual will be considered misleading and inherently unfair if the personal data would still be processed on a different lawful basis if the consent was refused or withdrawn – as this presents the individual with a false choice. It is worth noting that relying on consent where it is not appropriate or invalid could lead to substantial fines under the GDPR.

Consent is only one of the grounds on which personal data can be processed under the GDPR. In order for a consent to be valid: (i) it needs to be freely given; (ii) the individual must be able to refuse or withdraw their consent (without detriment); and (iii) the individual must have a genuine choice and control over how the data is used.

It is important under GDPR to be clear as to the basis for processing, and GDPR's enhanced requirements should be prompting HR to understand how data flows through your department, and why this is required. Consent should not be the default option, and in fact will be the exception rather than the rule. Instead, consider if processing is needed:

— for performance of the employment contract;

— in order to comply with legal obligations;

— to protect the vital interests of the employee or of another natural person (including the employee's dependents or family); and/or

— due to legitimate interests of the Company (provided that such processing is proportionate to the interests and fundamental rights are freedoms of the employee or data subject).

What does this mean for employers?

— Clauses in contracts of employment relying on consent should be reviewed and, if being kept, updated to reflect an alternative basis for processing.

— If you do not already do so you should issue employees and other personnel with a data privacy notice (we will discuss this in more detail in one of our next GDPR Bitesize updates).

— Where consent is needed, in one off situations or where the other grounds do not apply e.g. where an employee authorises earnings details to be sent to their bank for a mortgage application, ensure that it meets the strict requirements under the new regime.

Getting to grips with Employee Data Privacy Notices

As part of GDPR compliance, data subjects need to have a very clear explanation of how their information is processed, in the form of a Data Privacy Notice (DPN) (sometimes known as fair processing notices). HR teams will naturally be in the front line to produce these for those working in the business. In our experience the minority of employers currently issue DPN's in anything more than very brief terms, and this is therefore likely to involve a new rather than updated document/approach in most cases.

What has changed?

The GDPR requires more detailed information to be included in DPNs. Many employers have simply dealt with this issue until now through simple clauses in contracts which have set out quite generic information, and normally been combined with an attempt to document consent. Now, as a result of:

— the right to be informed of processing, and the requirement to be transparent and provide accessible information

— a new accountability requirement where employers have to be able to demonstrate compliance

— a move away from consent (see our last GDPR Bitesize)

— enhanced data subject rights;

a compliant DPN for the processing of employee personal data is essential.

Who should receive a DPN?

All those whose data is processed! In the context of HR teams the most obvious groups will be both job applicants and employees/workers, who should be issued with a DPN at the point the employer collects the personal data. So, for example, recruitment processes will require to be adapted to issue applicants with a DPN. Further DPNs may be needed when there is new or amended processing, not dealt with under the original.

What information should be included in a DPN?

The DPN must be concise, understandable and accessible. Information to be provided includes:

— the legal basis for processing;

— how long the personal data will be kept;

— if the personal data will be transferred overseas; and

— the data subject's rights.

DPNs must also explain whether data has been obtained by a third party source. For example, external medical information or pre-employment checks.

What should employers do now?

— Identify which groups you will need DPNs for and how/when you will deal with this.

— Update template DPNs or draft new ones.

— Train HR staff on the need to understand the legal basis for processing and to ensure that there is fair processing in line with the DPN.

The ICO explains that providing a privacy notice does not by itself mean that the employer's processing is fair. Employers also need to consider the effect of their processing. HR teams should remember to review the legal basis for processing at the start of different projects where they are processing new categories of data or processing existing data for a new purpose, particularly special category (sensitive) personal data (e.g. criminal records, medical information, information about sexual orientation) in order to ensure that the DPN covers this processing.

Time to update your subject access procedures

The data subject access request ("DSAR") has always been a central pillar to data protection legislation, providing individuals with a means of checking whether their data is being processed lawfully. The GDPR greatly enhances existing data subject rights, and provides a harsher potential penalty for an employer's non-compliance – with breaches assessed against the upper tier of potential fines.

What will change under GDPR?

Staff will still be able to ask for copies/details of their personal data, and the right to ask for inaccurate information to be rectified will continue. However, internal DSAR procedures should now be updated to refer to the changes e.g.:

— Employers will have to respond to DSARs without charging a fee (unless the request is excessive or unfounded).

— The response to a DSAR must be quicker than before – within 1 month (extendable in certain limited circumstances – understanding how to assess and operate this extension may be key to success in more involved cases).

— In addition to the usual background information given to the requester regarding the processing of their data, additional matters must now be confirmed relating to data retention periods, safeguards for data transfers outside the EEA, and the right to complain to the Information Commissioner's Office.

Other potential right are to have data made "portable" (and transferred to another organisation), or to have such data erased or restricted (i.e. not processed further), however we expect these to have far less practical impact in most cases for employers, due to the limited circumstances in which those rights will apply.

These data subject rights should be summarised in an employer's data privacy notice to staff.

What steps should employers take to prepare for change?

— Policy updates - Any policy referring to DSARs and/or Data Retention Policies should be updated.

— Training – Those staff most likely to deal with DSARs should receive training on the updated legal regime and company approach to the various judgement calls that will be required.

— Audit and understand The draft Data Protection Bill currently provides that decisions made regarding restricting any DSAR rights have to be explained and documented in case of future audit. It is vital there is a rigorous and centralised process.

— Updated process - Finally, the processes/software involved in data gathering for DSAR responses must be considered. The GDPR requires that the design, development and selection of any application or product that processes personal data should have privacy considerations at its heart through a system of data protection "by design and default".

The ICO is clear DSARs have been a part of life for over 30 years and employers are expected to have processes and systems set up to enable meaningful responses. With the perfect storm of GDPR publicity and general increased awareness (and exercise) of data subject rights generally, there will be nowhere to hide on subject access in future.

Data subject rights

Data subjects have always had the right to make subject access requests. When the GDPR comes into force, data subjects will have additional rights, which will have significant practical consequences.

Custodians of data?

Employers need to change the way they think about employee data. GDPR shifts the onus to make clear data controllers (in this case employers) are custodians of their data subjects (their employees') data. If employers apply this approach, the enhanced data subject rights given to employees can seem a more natural consequence, with employers adopting what may be described as a "caretaker" role.

What are the enhanced Data Subject Rights?

- **The right to be informed** – employees have the right to be provided with clear, transparent and easily understandable information about how employers will use their personal data, and their rights.
- **The right to correct or erase information (the right to be forgotten)** –
  - where employers hold personal data that is inaccurate or incomplete, employees have the right to ask employers to rectify or complete this;
  - where personal data has been processed unlawfully, or where it is no longer necessary for the purpose(s) for which it was collected, or where the employee objects to processing (see below) and there is no overriding legitimate interest for continuing to process the personal data, the employee may ask their employer to erase it. This right is not an absolute right, however, and employers can, for example, refuse a request where they need to process the data to exercise or defend legal claims.
- **The right to restrict processing** – employees have the right to restrict processing of their personal data by asking their employer to limit what they do with it. Where an employee disputes the accuracy of personal data held by the employer or the legitimate interests on which the employer considers that they can process the data lawfully, the employee may ask their employer to restrict processing for the period of time they need to verify that accuracy or to check that their legitimate interests override the employer's interests. The employee may also restrict processing where processing activities are unlawful or where an employer no longer needs the personal data, but they would like it retained to ensure its continued availability in connection with any legal claims.
- **The right to object to processing** – employees can object to processing under certain circumstances. Where this happens, the employer must stop processing the employee's personal data unless they can show that their legitimate ground for processing the employee's personal data overrides the employee's interests or where the employer needs to process the data to establish, exercise or defend legal claims.
- **The right to data portability** – employees have the right to obtain and reuse personal data for their own purposes. This only applies in a limited set of circumstances and we expect will have far less relevance for HR teams than the other rights. It only applies where processing is carried out by automated means, to personal data that the employee has provided (i.e. not any other information) and where processing is based on the employee's consent or for the performance of a contract. The employee can ask their employer to send them electronically the personal data or to a third party of their choice. Employers can refuse a request if the personal data concerns more than one individual and transferring the personal data in question would prejudice that person's rights.

— **The right to object to automated decision making** – Employees have the right not to be subject to automated decision making where this has legal or other significant consequences, except where the employee has explicitly consented to this or where it is necessary for entering into or performing a contract.

What does this mean for employers?

These are not simply conceptual rights. There are a number of practical consequences flowing from them, which include:

— The employer's HR data audit should identify areas of data which is past its shelf life. Ideally employers would carry out a data cleanse, to avoid issues arising under the new rights, recognising however that for many employers this would be a huge exercise.

— Data subject rights should be set out in the privacy notice issued to employees, with appropriate tailoring. For example, if you do use automated decision making as part of your recruitment process can you either obtain effective consent or demonstrate that this is necessary for the performance of the contract?

— DSAR response templates should also set out the list of enhanced data subject rights, with these also featuring in an updated data protection policy.

— HR, legal and IT staff should be trained on and aware of how to deal with these rights in practice.

Effective enforcement and painful penalties: are you up to speed with the new GDPR breach reporting process and enforcement regime?

By now most of us are aware that the GDPR is coming into force in May 2018, and this will involve a range of new duties and obligations on employers. Among the changes is a new duty to self-report data breaches - and the potential penalties for failing to do so, or for committing any other serious breaches of the GDPR, are eye-watering. Data breaches can also have wider reputational and financial consequences. Recently, Morrisons was held vicariously liable for the actions of an employee who deliberately disclosed personal information about its staff. Over 5,000 employees are claiming compensation for the distress caused by their salary details being posted online.

Breach reporting under the GDPR

No one likes to report their own wrongdoing. Yet the risk of not doing so is now higher than ever. Once the GDPR is in force, data controllers and data processors will need to notify the ICO of all data breaches without undue delay. A data breach is:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The timescale for reporting such a breach is 72 hours from becoming aware of the default, which could be a tall order if you happen to find out about it at 5:00pm on a Friday. Any delay will require a convincing 'reasoned justification' to the ICO the bar for this is likely to be set high. It's also important to note that for the first time data processors will also be required proactively to notify the data controller of their data breaches. A notification to the ICO can however be avoided where the breach is unlikely to result in a real risk to the data subjects concerned. Assessing whether that is the case will need careful, case-by-case analysis.

In addition if the breach is serious and is likely to result in a high risk to the rights of the data subjects (employees in an employment context), then the data controller (the employer) must also communicate the personal data breach to the individuals concerned without undue delay.

Enforcement and penalties

Inevitably there is one question all business stakeholders want to know when a legal breach has been identified – how much are we on the hook for?

Under the current regime, the ICO can impose a fine on data controllers of up to £500,000. However, the penalties under GDPR have the potential to blow this out of the water. For "Tier 1" data breaches (those of a most serious nature), the ICO will be able to impose a financial penalty of up to €20million or 4% of worldwide annual turnover (whichever is the higher). For less serious "Tier 2" breaches, the cap is reduced to the not insubstantial €10million or 2% of worldwide annual turnover. These are in addition to a host of other options open to the ICO, including criminal prosecution and non-criminal enforcement action (e.g. data protection audits).

Quite aside from any action taken by the ICO, there is of course also the issue of the brand damage that can result from a publicised data breach, not to mention any internal reputational harm where an HR team is identified as the responsible party. Brand damage could be particularly harmful in sectors such as health and

information technology, where data protection is an important perennial issue. It is crucial for clear rules to be set and disciplinary action to be taken appropriately in order to achieve a culture of compliance in which individual and organisational data protection responsibilities are taken seriously by all.

How would your security processes deal with a rogue employee?

An important factor to consider in light of the Morrisons case mentioned above is whether your organisation is sufficiently protected from rogue employees. If an employee in your business wanted to bypass security procedures, how easy would this be? Most data security breaches involve accidental human error. However, the Morrisons case was different because the employee deliberately leaked data. The ruling of the case creates an additional layer of risk for employers.

Morrisons was held vicariously liable for the actions of an employee who had disclosed the personal information of around 100,000 colleagues on the internet. While the disclosure had taken place outside working hours and from the employee's personal computer, the High Court considered that there was a sufficient connection between the position in which he had been employed and his wrongful conduct to make it right for the employer to be liable.

Criminal prosecutions for breach

We have also seen a recent case of the ICO bringing a criminal prosecution against a charity employee (rather than the charity itself) for a data breach, highlighting the tougher stance the ICO is already starting to take – even in relation to individuals. This trend looks set to continue once the GDPR comes into force, given the focus it will put on the ICO acting consistently with other countries' often much stricter regulators.

What steps should HR teams take to plan ahead?

— The ICO has highlighted that it expects organisations to be taking action now to review the roles, responsibilities and processes in place for breach reporting. There are detailed formal notification requirements that need to be followed. Organisations will need to have a data breach register and formulate a data breach response plan to enable them to respond promptly to a breach.

— It would be advisable to link in with your IT and risk teams to discuss whether there are any additional security protocols which should be put in place to minimise the risk of rogue employees.

— HR teams should be trained on the new rules regarding data breaches and the organisation's internal response plans.

February 2018

Contact Details

If you would like to discuss any of the issues raised in this document or for further assistance with your GDPR compliance plan, please contact your usual CMS contact or one of our employment partners below.

Alison Woods
Partner
T +44 1224 267176
E alison.woods@cms-cmno.com

Anna Cope
Partner
T +44 20 7067 3455
E anna.cope@cms-cmno.com

Catriona Aldridge
Partner
T +44 131 200 7350
E catriona.aldridge@cms-cmno.com

Gary Henderson
Partner
T +44 20 7071 7320
E gary.henderson@cms-cmno.com

Hannah Netherton
Partner
T +44 20 7067 3634
E hannah.netherton@cms-cmno.com

Steven Cochrane
Partner
T +44 20 7367 3746
E steven.cochrane@cms-cmno.com

Melanie Lane
Partner
T +44 20 7067 3653
E melanie.lane@cms-cmno.com

Catherine Taylor
Partner
T +44 20 7067 3588
E catherine.taylor@cms-cmno.com

Finlay McKay
Partner
T +44 131 200 7632
E finlay.mckay@cms-cmno.com

Gillian MacLellan
Partner
T +44 141 304 6114
E gillian.maclellan@cms-cmno.com

Richard Brown
Partner
T +44 20 7524 6051
E richard.brown@cms-cmno.com

Tracey Marsden
Partner
T +44 114 279 4114
E tracey.marsden@cms-cmno.com