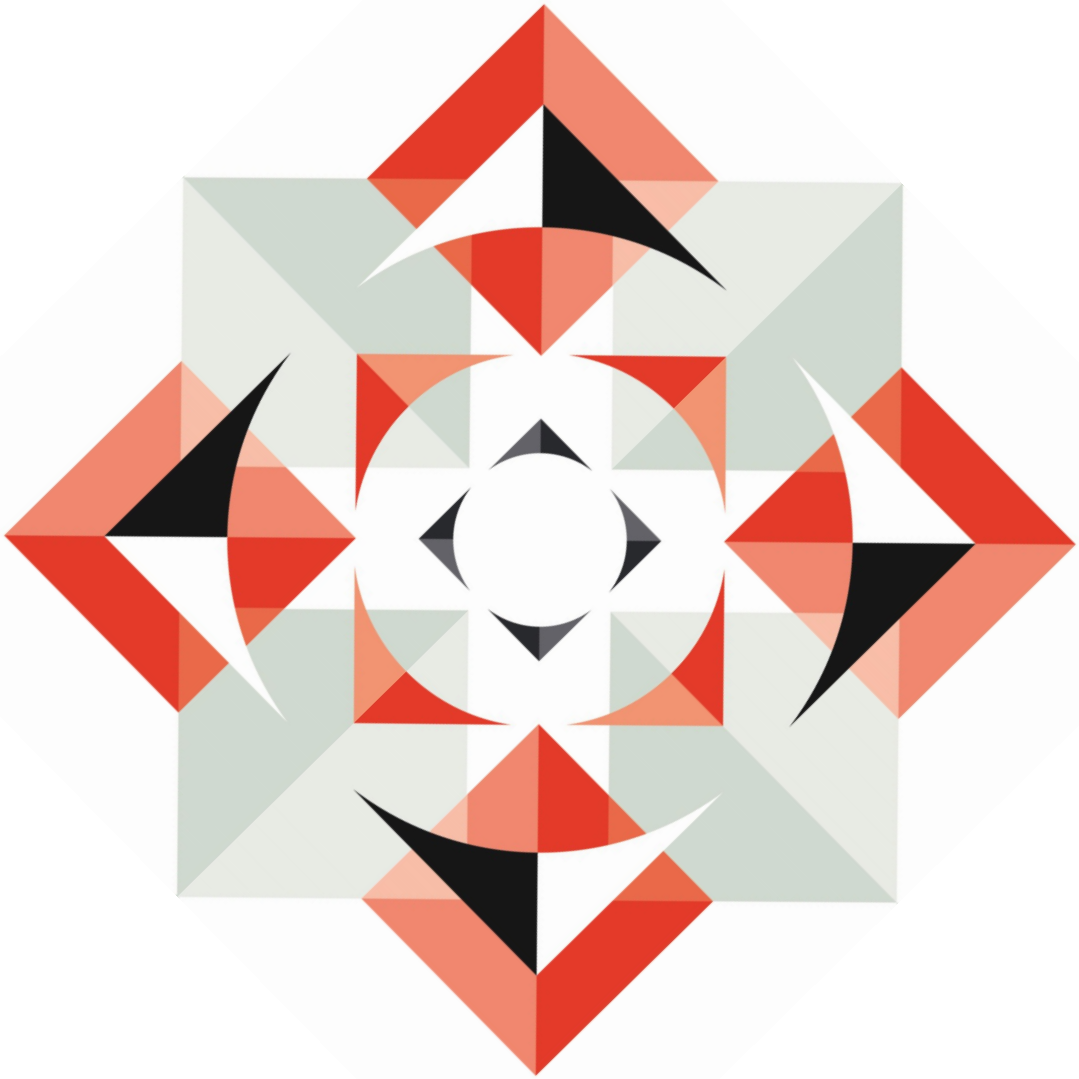
Ius Laboris UK Global HR Lawyers
LEWIS SILKIN

# General Data Protection Regulation: 11 steps to take



Inside

## Introduction

The data protection landscape has changed. The EU General Data Protection Regulation ("GDPR") came into force on 25 May 2018. The GDPR has introduced a number of changes to data protection law including:

> expand the territorial scope of data protection laws;

> increase the penalties for transgressions from a maximum of £500,000 under the old law to up to €20,000,000 or 4% of worldwide turnover, whichever is higher; and

> radically change the processing, recording and other compliance obligations of businesses.

British businesses can't count on Brexit to let them off the hook. The GDPR is directly applicable law until the UK leaves the EU. Even after Brexit the regime will remain in force through the Data Protection Act 2018. It seems then that the new data protection regime is here to stay.

Lots of businesses have already made major changes in order to navigate the new data protection landscape, but some are still in the process of getting their compliance programme in place. We've set out here some key things to consider in the post-GDPR world.

### 1 Determine what workforce data you process and why, where you send it and who you share it with.

This is the first step most organisations will need to take. It will help to inform decisions about the legal basis for processing such data, will assist therefore in the completion of privacy notices to meet transparency requirements, will enable you to locate data to comply with data subject rights, and provide the information you need to complete the records of processing which the GDPR mandates both processors and controllers maintain.

To do this you should conduct a data-mapping exercise, a process that shows how data from one information system transfers to another, and an audit. Audits assess your data protection practices by looking at whether you have effective policies and procedures in place, whether you are following them and identifying where improvements could be made.

### 2 Are your third-party processors compliant? Review arrangements with third-party processors

The GDPR imposes more onerous obligations to ensure that the right contractual guarantees are in place when organisations appoint data processors, so these agreements should be reviewed and overhauled as part of the audit process. You should start by identifying your data processors, such as payroll providers, and reviewing the contractual terms. Your audit should review what due diligence you have in place to vet third-party processors prior to appointment and check that the written agreements you have with them meet compliance requirements. Where they do not, you need to put in place terms which include the requirements set out in the checklist.

Compliance checklist for an agreement with third party processors

Under the GDPR, the agreement must:

> Set out the subject-matter, duration, nature and purpose of the processing, type of data, categories of subjects, and obligations and rights of the controller

> Stipulate that the processor must:

- process the personal data only on documented instructions from the controller
- ensure that persons authorised to process the personal data have committed themselves to confidentiality
- comply with data security obligations
- not engage another processor without consent (and ensure any sub -processor commits to the same contractual obligations)
- assist in fulfilling data subject rights requests through appropriate technical and organisational measures
- assist the controller with certain obligations including data security and the obligation to undertake impact assessments
- delete or return all the personal data to the controller after the end of the provision of services
- make available to the controller all information necessary to demonstrate compliance and allow audits by the controller

Where you share data with other controllers, you should also examine the protocols in place; you may not need a formal agreement in all cases with other controllers but you should conduct due diligence and assess risk. Where you act as a joint controller some written terms will be desirable to apportion responsibility for compliance between controllers.

Businesses should also think about how they deal with independent contractors / freelancers, agency workers, and secondees. This is a complex issue but thought needs to be given to the contractual terms necessary to protect any data that they may handle while they have access to your systems. The first question is what type of service they provide; some will act as independent controllers but many contractors who are "quasi" employees are likely to be data processors, meaning agreements with them should contain the above terms, although in some circumstances, that may seem a little unwieldy. In any event a risk assessment should be undertaken. Agreements will need to be tailored slightly where the contractor / freelancer operates through a personal service company ('PSC') as in such a case the PSC (rather than the individual) will be the data processor.

### 3 Establish a cross-border inventory of data flows and check that the transfers are covered by appropriate arrangements

Catalogue your cross-border workforce data flows, and consider your approach to overseas transfers in light of recent developments such as the EU-US Privacy Shield (the current framework for exchanges of personal data between the USA and the EU, replacing the Safe Harbor principles), challenges to model clauses (EU-approved contractual clauses which can be put in place between the data exporter and recipient ensuring protection of the data) and the UK's eventual relationship with the rest of the EU.

Ensure that data which is transferred outside the EEA is transferred pursuant to an arrangement which ensures adequacy requirements are met. You may need (for example) to put in place the EU model clauses, BCRs or just consider whether transfers are justified by one of the "ad hoc" grounds for transfer permitted by the GDPR. These requirements will need to be met even intra-group for transfers to affiliates overseas.

### 4 Appoint a data protection officer

Companies whose core activities consist of processing operations that require (a) regular and systematic monitoring of data subjects on a large scale or (b) large scale processing of special or criminal data have to appoint a data protection officer. This must be a person with expert knowledge of data protection law and practices, whose job is to monitor internal compliance with the GDPR. This person has to be independent and will gain a number of workplace protections, similar to a Trade Union or Works Council representative.

Even if you are not required to appoint a data protection officer, we would recommend appointing somebody within your organisation to monitor any data processing to ensure that it complies with your GDPR obligations, given the potential level of fines under the new regime. Although in these circumstances it is best not to call them a 'data protection officer', as this would mean that even if they are not a mandatory data protection officer they could get all of the same rights and protections.

### 5 Don't rely on consent to justify your processing (where possible)

Many employers have historically relied on employee consent to justify all their workforce data-processing activities, by including a clause in the employment (or freelancer) contract at the outset of the relationship. This is problematic under the GDPR, which incorporates the long-held view of the European regulators that consent to processing in the context of a contractual employment relationship cannot be considered as freely given.

Under the GDPR, consent must be actively and freely given to be a valid basis for data processing – silence or inactivity do not count. The GDPR also states that where consent is given in a written declaration that also deals with other matters, the request for consent must be clearly distinguishable from those other matters and in an intelligible and accessible form. It must be as easy to withdraw consent as it is to give it, and if there is a clear imbalance between the parties, such as in an employment relationship, consent is presumed not to be freely given. It is clear from all these factors that signing an employment contract with a general consent clause cannot amount to freely given consent. Moreover, typically, insufficient information is given in employment contracts to meet fair-processing requirements.

Another reason to move away from consent as a basis for processing is that it triggers certain rights on the part of the employee. For example, employees are able to retract their consent at any time, preventing data controllers and processors from processing their data.

Fortunately, consent is only one of a number of valid conditions for processing personal data. Conducting an audit will enable you to identify the various types of workforce personal data you need to process in the course of the employment relationship and you will be in a better position to find another valid basis for the processing. To take a straightforward example, employees' bank details are needed to pay salary but this processing can be justified on the basis that it is necessary for the performance of the contract rather than through consent. Another example would be monitoring employees' use of IT systems for data security reasons. Seeking consent to do this could cause problems, as it might be withheld or revoked. Instead, you could justify the processing on an alternative ground, such as your legitimate interests (depending on the reasons for the monitoring), or your legal obligations to maintain the security of the data that you handle. Similarly, performance management data about employees could be justified for the purposes of legitimate interests pursued by the data controller.

Employers should rely more heavily on these alternative bases for processing data. On the rare occasion where it remains necessary to obtain consent to process data, employers should consider carefully what specific information they must provide to the data subject when seeking consent. Where consent is obtained, it must be given actively, separately and freely – and the employer must be able to evidence compliance.

Whilst employers may move away from having a general, all-encompassing, "data protection" clause in the employment contract, there are some data protection related contractual clauses they should retain – in particular, ensuring that employees are aware of their own responsibility to process personal data properly and the consequences of failing to do so. Other policies (such as "bring your own device" and data security policies), training rules and disciplinary procedures should also be double-checked to ensure that they address the issue of employee accountability.

### 6 Adapt your privacy notices and policies

Under the GDPR, data subjects are entitled to receive a lot more information about their data and how it is handled than under the previous regime. This "fair processing information" includes information about who has access to the data, why, how long it will be held for, and their rights. This means that you will have to spell out the rights of the data subject – such as the right to withdraw consent to data processing and to lodge a complaint with the ICO.

The notice must specify the purpose and legal basis for processing each category of personal

data, and this should be informed by the audit you have undertaken (see above). If they haven't already, pre-GDPR privacy notices for your workforce will need to be considerably revised. You may want to develop a main privacy notice for your workforce and a separate one dealing with recruitment data.

## 7 Set up systems to deal with data subject rights

The 40-day time limit for responding to data subject access requests ("DSARs") has now been reduced to one month. If requests are complex or there are a number of requests from the same source, this limit can be extended by a further two months although the controller needs to write within the first month explaining whether he will comply or not and whether he intends to take advantage of this extension. The £10 fee has been scrapped. A 'reasonable fee' can be charged if the request is manifestly unfounded or excessive.

Pre-GDPR guidance from the Information Commissioner's Office ("ICO") already recommends that you have a process which logs and tracks DSARs. You may need to introduce such processes if you do not already have them and expand existing processes to address the other data subject rights, which include, subject to certain exemptions:

- a right to have inaccurate data restricted
- a right to erasure of personal data in certain circumstances, such as where there is no longer a purpose for the processing, or where consent is withdrawn and there is no other valid legal basis
- a right to restrict (freeze) processing in certain circumstances, such as where the subject has contested accuracy or objected
- a right to receive data in a machine-readable format
- a right to object to an act of processing based on the controller's legitimate interest.

Responding to DSARs in particular is often complex and you should train appropriate individuals to handle them, to apply consistent principles when making objections (such as objecting to the request as "unfounded" or "excessive") and to ensure that third-party data is handled appropriately. Depending on the size of your organisation, this may be one person or a team, most typically in HR or Legal. Data subjects also have a right to access more information about how their data is processed under the GDPR and so you should review any existing training provided to those handling requests to ensure that you remain compliant.

## 8 Work towards "Privacy by Design"

The GDPR requires organisations to implement policies, procedures and systems at the outset of any product or process development to ensure data protection compliance ("privacy by design"). Privacy impact assessments are required where there is a high risk to the rights and freedoms of data subjects, in order to establish whether any proposed processing is reasonable in the circumstances. Some HR activities may fall within those regarded as high risk.

As a general rule, recording how you balance the conflicting interests and rights of data subjects against your business's rights or those of other data subjects is a central theme of privacy compliance. Impact assessments which record how you arrived at a particular decision are recommended.

## 9 Data breach management

Organisations have to notify relevant data breaches to a supervisory authority within 72 hours. You should therefore give very careful thought to breach prevention and ensuring that any breaches are handled in the right way. This involves raising awareness of data handling issues, training staff on appropriate behaviour and ensuring staff know what they need to do in the event of a data breach. If you don't already have one, having a clear data breach protocol for employees to follow is recommended. It will also be necessary to implement joined-up training across multinationals, as a breach may concern more than one jurisdiction.

## 10 Training

This has already been mentioned but it deserves a heading in its own right – key topics are data awareness, data security, and subject access. The entire workforce should be trained in data awareness and you should record who has received it. Those with specific responsibilities to handle personal data should receive enhanced training.

## 11 Consider your post-Brexit position

Non-EU established businesses who offer goods and services or monitor subjects in the EU must designate a representative in one of the EU member states with whom regulatory authorities can liaise. As the UK prepares to leave the EU, businesses without an EU establishment will need to think about who to appoint once Brexit takes place.

Where businesses are established in more than one EU member state they may need to consider whether to take steps to appoint a lead regulator. The lead regulator is the supervisory authority in the country where the controller/processor has its main establishment. Once the UK leaves the EU, as a non-EU controller or processor, a nomination may be made by a group of companies as to whom the main establishment within the EU will be.

## Conclusion

With the GDPR now in force, if you haven't already done so, you should be making the necessary changes to your processes, policies and other documents so that your business will be compliant.

For further information on this subject please contact:

**Ellen Temperton**
Partner
**T** + 44 (0) 20 7074 8424
ellen.temperton@lewissilkin.com

**Alexander Milner-Smith**
Partner
**T** + 44 (0) 20 7074 8196
alexander.milner-smith@lewissilkin.com