LEWIS SILKIN

Data & Privacy: 8 key ways to Prepare for GDPR

Introduction

Significant changes are coming to data privacy regulation. The EU General Data Protection Regulation ("GDPR") will directly apply to all European Union member states from 25 May 2018, which at that time will still include the UK. Elizabeth Denham, the UK Information Commissioner has said: "I acknowledge that there may still be questions about how the GDPR would work on the UK leaving the EU but this should not distract us from the important task of compliance with the GDPR by 2018".

Even once the UK has withdrawn from the EU, the UK must still offer 'adequate protection' by EU standards to avoid being designated as inadequate in terms of the level of protection afforded to personal data – and to ensure that international data flows between the UK and the rest of Europe continue to be lawful.

In any event if you have operations in the rest of Europe or you offer services (or goods) in other European Member States, you will need to comply with the GDPR.

Read on for some key tips on how to practically prepare…

1. Map and audit your data flows and processes

You should conduct a data-mapping exercise (a process that shows how data moves from one information system to another) and an audit. The audit process will asses your data protection practices around those flows of information and look at whether you have effective policies and procedures in place and identifies where improvements should or could be made.

These exercises will determine what personal data you process and why, where you store and send it and who you share it with. This will help you check you're complying with current and future regulations and inform decisions about the basis for such processing in the future, as well as help you prepare for the new record-keeping obligations within the GDPR. An audit will help your organisation identify areas of risk and help you prioritise what changes need to be made before GDPR applies.

2. Check your data processing

You'll need to identify third parties who also handle personal data for you and consider if they are processors (acting purely on your behalf) or also controllers. Review the contractual terms, which need to be *in writing* under both current and future rules. The GDPR imposes more onerous obligations around the *detail* of data processing agreements and you need to ensure that the right contractual guarantees are in place where you appoint *processors*. If you're sharing data with another *data controller* you should also examine the protocols and contracts in place for those relationships too.

3. Review your cross-border data flows and consider your regulator

Chances are, some of the data you deal with will cross borders. If that's the case you will need to establish an inventory of the data flows and consider your approach to those transfers – including any which are overseas. Recent developments (such as the EU-US Privacy Shield and challenges to EU approved Model Clauses) mean you'll need to check that what you're doing is compliant and keep an eye on these relationships as the UK withdraws from the EU.

In addition, the GDPR introduces a new concept of the "lead regulatory authority" who will deal with complaints and sanctions where your organisation is processing data across EU-borders. Your lead regulator will be the country where the controller or processor has its *main establishment* and this can vary depending on the type of data involved (for example one group of companies might centralise its marketing function in the UK, but run all its supply and procurement relationships from France).

A non-EU controller or processor can nominate a main establishment within the EU so once the UK leaves the EU this might become relevant to your business too, and you'll need to consider carefully which country that should be in your particular case.

4. Think about why you're processing personal data

As with the current law, you need to consider the grounds on which you justify your data processing, for example will you rely on: consent from the individual; or the argument that the processing is necessary for the particular contract; or even that it's in your legitimate interests? Think carefully about which you rely on - this will obviously depend on the type of data you're processing and why (which if you've done a data mapping/audit exercise, will hopefully be clear.…).

If you rely on *consent*, this needs to be fully informed, actively and freely given. Consent won't be valid if you've hidden the details about why you're processing within a long set of terms and conditions and if the individual doesn't really have a choice about the processing. Remember that consent can be withdrawn at any time, so it may not be a practical ground to rely on.

Particularly in an employment context, consent is not going to work as the GDPR has made clear that consent by employees won't be valid. So you will no longer be able to rely on employee consent in an employment contract at the outset of the relationship to justify all workplace data-processing activities and you will need to consider the alternative grounds to rely on.

5. Review your privacy notices and polices

A key concept under the GDPR is '*transparency*' and this continues the existing requirement to provide individuals with a "fair processing notice". Data subjects, i.e.the individuals whose data you process, will be entitled to receive more information about their data and how it is handled, including who has access to it, why they have access to it, for how long it is held and the rights that they have in relation to it. This means you have to spell out the rights a data subject has – such as the right to withdraw consent to data processing (if that's the ground you're relying on) and to lodge a complaint with the ICO.

Privacy notices will now need to specify the purpose and legal basis for processing each category of personal data, and this should be informed by the audit which you have undertaken (see above). Existing privacy notices – both externally facing from your business, and the policies provided to your workforce, will need to be reviewed and may need to be revised considerably.

6. Work out how you'll deal with the new data subject rights

In addition to continuing the right for all data subjects to make 'access requests' and be given details of what personal data is being processed, the GDPR introduces some additional, and more detailed, rights for data subjects including a right to data portability and the right to be forgotten.

While some of these rights don't apply to all data, they cannot be ignored and it is likely, bearing in mind the new 'transparency' requirements mentioned above, that you might begin to receive requests even if you haven't had similar requests before. You will need you to review and consider internal and external-facing processes as to how you deal with requests and consider which are most likely to arise in your business. For example, subject access requests might come from employees or third parties whose data you process so you'll need to have appropriate procedures in place for both and train your staff to follow those policies.

7. Prepare, prepare and preparesome more for data breach!

The GDPR introduces mandatory data breach notifications to the *regulator* within 72 hours and in some cases to the *data subjects* too. Unless your business is already subject to the E-Privacy breach notification requirements, you might not have a plan in place to deal with data breaches as notification has otherwise to date been voluntary.

Organisations need to give very careful thought to breach prevention and ensuring that breaches are handled in the right way to avoid non-compliance, as well as the business and PR issues resulting from a data breach.

Your approach should take into account how an actual breach will be handled and who else you will need to involve within your business and in terms of external advisors, and you will need to raise awareness amongst all your workforce and train staff as to appropriate behaviour and procedures. It is also necessary to implement a joined up approach across *multinationals*, as a breach may concern more than one jurisdiction.

8. Appoint a DPO

C ompanies whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale will now have to appoint a data protection officer. This must be a person with expert knowledge of data protection law and practices, whose job will be to monitor internal compliance with the GDPR. You'll need to consider carefully if this applies to you and think about who could perform the role, or if you need to recruit. Note that a key concept of the DPO is that they are *'independent'* so a CEO, Finance Director, CISO or Marketing Director can't also hold the role.

According to guidance from the group of European data regulators (the Article 29 Working Party), "core activities" won't include support functions such as HR and payroll but will include data collected as an inextricable part of the pursuit of your business goals. For example, customer data for an online retailer is likely to be core. 'Large scale' itself hasn't been defined but factors to consider include the number of individuals monitored, the geographic extent and permanency of the personal data collected and the volume or range of data processed.

And 'regular and systematic monitoring' *includes* internet tracking and profiling for the purpose of behavioural advertising, providing telecoms services, credit and risk assessment, location tracking, loyalty schemes and the operation of smart appliances.

The GDPR will not be enforced until May 2018, but it is important to start thinking now about how to prepare. Guidance is emerging – slowly – from the European regulators and more is expected in late 2017 and early 2018. The GDPR will have legal direct effect on Member States, but as it does still include the ability for individual Member States to set some rules, it remains to be seen exactly how the UK will replace or amend the Data Protection Act in terms of legislation. And if the GDPR wasn't enough of a change, the European Commission recently introduced a new draft E-Privacy Regulation (dealing with, amongst other things, collection of behavioural advertising, location data and 'cookies'). As a regulation this is also intended to have direct effect on EU Member States and an ambitious timetable of being negotiated and agreed so that it can come in force at the same time as the GDPR. Watch this space!

For further information on this subject please contact:

Nick Walker
Partner
T + 44 (0) 20 7074 8055
nick.walker@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com