STEPHENSON HARWOOD

The GDPR countdown

What do you need to do?

The European General Data Protection Regulation ("**GDPR**") comes into force with direct effect in the European Union on 25 May 2018 and heralds a step change in data protection ("**DP**") law throughout the region. The GDPR is also due to be implemented into UK law through the Data Protection Bill (which was introduced to the House of Lords on 13 September 2017) so the UK will continue to meet its DP obligations after Brexit. But what does this mean for your business?

To ensure compliance with the new DP law by 25 May 2018, it is vital that organisations:

- take stock of their current DP practices now
- understand the impact of the changes to DP law for them and on their business
- take any necessary action.

Where to start?

Here. This document sets out an essential eight point DP checklist. The starting point for organisations that handle personal data should be a data audit, as this will go some way towards satisfying the new requirements and help identify what other steps they need to take. This should be undertaken as soon as possible to ensure full compliance by May 2018.

Key points for organisations to address in this process are:

- Privacy notices (additions will be required to ensure they meet the new requirements).
- A review of policies and procedures in light of the heavier penalties that may apply for non-compliance with DP legal requirements.
- A review of the legal bases adopted for processing personal data, including special categories of personal data.
- Shorter timeframes for complying with subject access requests and reporting any data breaches to the Information Commissioner's Office ("**ICO**").
- New and enhanced data subject rights in relation to personal data.
- Reviewing third party service provider agreements to ensure compliance with the new DP requirements.
- Negotiations with service providers over the extent of their liability for DP law breaches and any indemnities required.

Stephenson Harwood can help companies navigate their initial data audit and address the above points. Full contact details of our team of experts are on the last page of this document should you wish to find out more about our range of experience providing DP advice or should you have any general DP queries arising from this document.

1. Information held by organisations

Under existing DP law, there is an implicit requirement that data controllers know what data they hold and how that data is held. The GDPR makes this explicit, requiring data controllers to record and document details including the data they hold, the purposes for processing that data and who the data is shared with. Processors must also document their processing activities.

By doing this, organisations may discover certain DP issues that need to be addressed. For example, controllers may identify certain data that is not necessary and make arrangements for its deletion.

To comply with this new requirement, organisations should consider carrying out a data audit covering:

- **the personal data held**
- **the source of that data**
- **how the data is stored, where it is stored and how long for**
- **the reason(s) it is necessary to process that data**
- **whether it is lawful to process that data**
- **who else has access to the data.**

2. Communicating privacy information

Data controllers should already use privacy notices that provide fair processing information to data subjects such as employees and customers and that might also seek express consent to the processing of personal and sensitive personal data.

The GDPR enhances the existing requirements so that it will be necessary for data controllers to communicate additional information to its data subjects, including:

- The reason(s) and the legal basis which they are relying on to process personal data.
- Data retention periods or criteria for how long data will be held.
- Information about data subjects' rights including the right to complain to the ICO where individuals think there is a problem with the way their data is being handled.

All notices must be concise, transparent, intelligible and easily accessible.

Controllers will need to review their existing privacy notices and update them in line with the new requirements.

3. Data rights (including subject access requests)

The current DP law already provides certain rights to data subjects (such as employees and customers) over the personal data that a data controller may hold about them. This includes a right to access their personal data and rights to stop certain data processing.

The GDPR makes significant enhancements and additions to these rights, including a new right to delete personal data where continued processing is unnecessary (not just where damage or distress is caused) and a right to "data portability", which is the ability to request that certain data is transferred to a different controller.

In addition, the subject access request ("**SAR**") requirements are being made more onerous, so that:

- The time for compliance with any SAR is reduced from 40 days to one month.
- The ability to charge a £10 fee for a SAR has been removed.
- It is possible to refuse, or ask for a reasonable administration fee for, unfounded or excessive SARs but prescribed information must be provided to the data subject in such circumstances.

Organisations should consider how their procedures should change to comply with these enhanced rights.

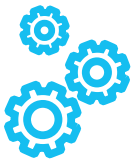
4. Data subject consent

Consent to the processing of personal data will generally become more difficult to obtain. For example, it must be freely given, specific, informed and unambiguous. There must also be a positive opt-in and so it will not be possible to infer consent from silence, pre-ticked boxes or inactivity. Requests for consent that are bundled in with other terms, rather than clearly separated out, will probably not be sufficient.

Data controllers that rely on consent to process data will need to review existing consents to determine whether they would be adequate under GDPR or whether there are more appropriate legal grounds to rely on than consent. Existing privacy notices in customer and employee contracts may not be adequate and so a new GDPR-compliant consent mechanism may be required.

Data subjects will have the right to withdraw consent at any time and this could potentially create significant operational issues for controllers. In addition, GDPR-compliant consent may be difficult to obtain by employers from their employees, since the imbalance of power means that consent may not be seen as having been freely given. As such, controllers may need to look for a different legal basis for processing personal data.

5. Legal basis for processing personal data



The legal basis (or bases) adopted for processing personal data will be more of an issue under the GDPR, as some individuals' rights will be modified depending on the legal basis adopted. For example, if controllers rely on consent, the data subjects will generally have stronger rights, including a right to have their data deleted.

Alternatives to data subject consent for non-sensitive personal data include where processing is necessary for the performance of a contract with the data subject or for the purposes of legitimate interests pursued by the controller (except where those interests are overridden by the interests, rights or freedoms of the data subject).

Data controllers need to determine the legal basis on which personal data is processed, document this and update the relevant privacy notices to explain it.

6. Accountability – demonstrating compliance

The GDPR includes an accountability principle which effectively means organisations must not only comply with the data protection principles but also demonstrate how they comply.

Organisations can take a number of steps to help ensure and demonstrate compliance:

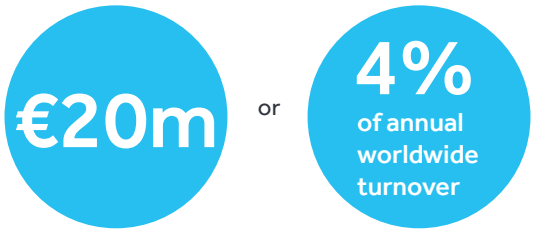
- Keep records of all data processing activities carried out.
- Implement (or review existing) technical and organisational measures for achieving compliance, e.g. data protection policies in relation to employee training and internal audits of processing activities.
- Undertake a data protection impact assessment ("**DPIA**") where data processing is likely to result in high risk to individuals, e.g. where new technology is being deployed. Data controllers could prepare a DPIA policy/template document.
- Implement measures that meet the principles of data protection by design and by default, including data minimisation, pseudonymisation, transparency, and improving security features on an ongoing basis.

7. Data breaches and fines for breaches

A personal data breach is a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

There will be a new mandatory requirement for controllers to notify data breaches to the ICO where it is likely to result in a risk to the rights and freedoms of individuals (e.g. where a breach could result in discrimination, damage to reputation or financial loss). Notifications must be made without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also notify the individuals concerned directly without undue delay.

Failure to notify can result in a fine of up to the higher of €10 million or 2% of annual worldwide turnover. Separately, higher fines may be imposed for the breach itself, which could be up to the higher of €20 million and 4% of annual worldwide turnover (a significant increase to the current maximum fine of £500,000).



Controllers' potential liability is therefore greatly increased. Data processors such as third party suppliers are directly responsible under the GDPR for informing the relevant controller "without undue delay" after becoming aware of a personal data breach, but controllers may wish to make this obligation more onerous under contract, by for example requiring that the processor notifies them within 24 hours, to give more certainty on timelines.

Controllers should ensure they have robust procedures in place to identify, assess, record and, where appropriate, notify data breaches. Controllers may also wish to revisit the protection from liability they obtain through indemnities in contracts with processors and any liability insurance.

8. Contracts with data processors

The GDPR places direct legal obligations on data processors in relation to things like implementing appropriate data security measures and keeping a record of processing carried out on behalf of a data controller. Data controllers and data processors are also required to ensure these contracts contain certain minimum provisions, such as a description of the scope, nature and purpose of processing.

Controllers should review and update their contracts with data processors to ensure there are appropriate provisions in relation to the data processor's new direct obligations and other relevant matters such as compliance, monitoring and reporting.

Liability and indemnity clauses in contracts should also be reviewed to ensure the risk allocation remains appropriate given that data processors now have direct legal obligations and given that data controllers and data processors will have the same obligations in areas such as security. Data processors will be directly liable for breaches under the GDPR and so may consider seeking indemnities from controllers in relation to data protection fines caused by the controllers.

If you would like further information on the developments referred to in this guide, our DP advice or any other data protection legal issues, please get in touch with your usual contact in the Stephenson Harwood data protection team.

Jonathan Kirsop

Partner

T: +44 20 7809 2121
M: +44 7554 403 022
E: jonathan.kirsop@shlegal.com

Caieta Hendry

Senior associate

T: +44 20 7809 2382
M: +44 7894 819 565
E: caieta.hendry@shlegal.com

Naomi Leach

Senior associate

T: +44 20 7809 2960
M: +44 7769 143 367
E: naomi.leach@shlegal.com

Alison Kenney

Associate

T: +44 20 7809 2278
M: +44 7557 162 343
E: alison.kenney@shlegal.com

Katie Samadi

Senior associate

T: +44 20 7809 2073
M: +44 7702 142 644
E: katie.samadi@shlegal.com

Katie Hewson

Associate

T: +44 20 7809 2374
M: +44 7702 141 048
E: katie.hewson@shlegal.com

Chloe Haywood

Senior associate

T: +44 20 7809 2348
M: +44 7872 112 799
E: chloe.haywood@shlegal.com

Anita Basi

Associate

T: +44 20 7809 2193
E: anita.basi@shlegal.com

David Berry

Senior associate

T: +44 20 7809 2269
E: david.berry@shlegal.com

Michelle Gomes

Associate

T: +44 20 7809 2370
M: +44 7872 106 630
E: michelle.gomes@shlegal.com

www.shlegal.com

STEPHENSON HARWOOD

BD285-GDPR-1017