STEPHENSON HARWOOD

The UK GDPR – an overview

What are your key obligations?

The General Data Protection Regulation ("GDPR") came into force with direct effect in the European Union on 25 May 2018 and heralded a step change in data protection ("DP") law throughout the region. The GDPR was implemented into UK law through the Data Protection Act 2018 and it continues to apply in the UK as domestic law following Brexit by virtue of the European Union (Withdrawal) Act 2018 as the "UK GDPR". But what does this mean for your business?

To ensure compliance with UK DP law, it is vital that organisations:

- take stock of their DP practices
- understand the impact of DP law on their business
- take any necessary action.

This guide is aimed at businesses that are reviewing their compliance with the UK GDPR and the GDPR in the UK, whether for the first time or as part of a regular update. Compliance is an ongoing process and it is important to ensure that your policies and processes stay up to date as your business develops.

Where to start with DP law compliance?

Here. This document sets out an essential nine point DP checklist. The starting point for organisations that handle personal data should be regular data audits, as these will go some way towards satisfying DP law requirements and help identify what other steps they need to take, or what updates are needed to existing compliance procedures.

Key points for organisations to address in this process are:

- Privacy notices (the UK GDPR contains prescriptive requirements as to their contents and they should be regularly reviewed and updated to reflect any changes to business practices since they were put in place).
- A review of policies and procedures in light of the heavy penalties that may apply for non-compliance with DP legal requirements, particularly as evolving market practice may be taken into account when assessing what steps organisations should take to comply.
- A review of the legal bases adopted for processing personal data, including special categories of personal data.
- The short timeframes for complying with subject access and other data subject requests and reporting any data breaches to the Information Commissioner's Office ("ICO") (or other competent authorities) and, where necessary, to data subjects.
- Enhanced data subject rights in relation to personal data.
- Reviewing third party service provider agreements to ensure compliance with DP law requirements.
- Negotiations with service providers and partners over the extent of their liability for DP law breaches and any indemnities required.

Stephenson Harwood can help companies navigate their data audits 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

The UK GDPR requires controllers to know what personal data they hold and how that data is used. Controllers must record, document and make available to data subjects details such as the personal data they process, the purposes for processing that data and who the data is shared with. Processors (i.e. those using personal data on a controller's behalf) 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. This exercise should be repeated at regular intervals, to ensure that any new processing activities are captured by the existing policies and to check that procedures are being followed.

To comply with this requirement, organisations should consider regularly carrying out and updating data audits 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. Communication of privacy information

Controllers should already use privacy notices that provide fair processing information to data subjects such as employees and customers.

It is important to ensure that these notices are up to date for all of the organisation's latest practices and that they include all of the detailed requirements in the UK GDPR in relation to the information that must be given to data subjects, including:

- The reason(s) and the legal basis on which they are relying 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 should review their existing privacy notices and update them in line with these requirements.

3. Data rights (including subject access requests)

Prior to the UK GDPR coming into effect, data subjects already had certain rights over the personal data that a controller holds about them. This included a right to access their personal data and rights to stop certain data processing.

The UK GDPR made significant enhancements and additions to rights that data subjects (such as employees and customers) have over the personal data that a controller may hold about them, including a 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 UK GDPR sets out onerous requirements for the exercise of all data subject rights, such as the right to object to certain data processing or the right to make a subject access request ("SAR"):

- The time limit for compliance with any request by a data subject to exercise their rights is one month from receipt.
- A data subject's request to exercise their rights need not be in writing or any prescribed format.
- 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 ensure that their procedures enable them to recognise and comply with these data subject rights in a timely way.

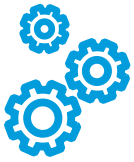
4. Data subject consent

Valid consent to the processing of personal data is difficult to obtain and demonstrate under the UK GDPR. It must be freely given, specific, informed and unambiguous. There must be a positive opt-in and so it is not 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, are not sufficient.

Controllers that have traditionally relied on consent to process personal data should have already reviewed existing consents to determine whether they would be adequate under the UK GDPR or whether there are more appropriate legal grounds on which to rely than consent. If an organisation is carrying out new activities based on existing consents, the consents will need to be checked to ensure that they cover the proposed new activities. To the extent that consent is relied upon as the appropriate legal basis, privacy notices in customer and employee contracts must be checked to ensure they are up to date and a UK GDPR compliant consent mechanism may be required to ensure that new consents continue to be properly obtained and recorded.

Data subjects have the right to withdraw consent at any time and this could potentially create significant operational issues for controllers. In addition, UK GDPR-compliant consent is 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 and document 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 under the UK GDPR can cause an issue, 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). If legitimate interests is the legal ground being relied upon, a legitimate interests assessment should be completed and documented.

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 UK 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:

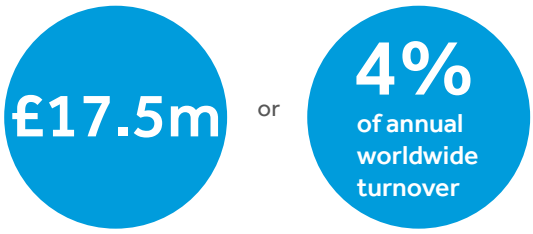
- Keep records of all data processing activities carried out and regularly review and update these records.
- Implement (or review existing) technical and organisational measures for achieving compliance, e.g. data protection policies in relation to employee training and internal audits of processing 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. Controller could prepare a DPIA policy/template document ready for use.
- 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, as activities, available safeguards and good market practice evolves.

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 is a mandatory requirement for controllers to notify data breaches to the ICO where a breach 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 £8.7 million (or €10 million under the GDPR) or 2% of annual worldwide turnover. Separately, higher fines may be imposed for the breach itself, which could be up to the higher of £17.5 million (or €20,000 under the GDPR) and 4% of annual worldwide turnover. Controllers and processors therefore carry significant potential liability.



Processors such as third party suppliers have their own UK GDPR security obligations and are directly responsible 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. The controller's 72 hours should however not start running until it is informed of a breach by its processor, where relevant.

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 processors

The UK GDPR places direct legal obligations on processors in relation to things like implementing appropriate data security measures and keeping a record of processing carried out on behalf of a controller. Contracts between controllers and processors must also contain certain minimum provisions, such as a description of the scope, nature and purpose of processing and a right for the controller to object to the appointment of sub-processors.

Controllers should review and update their contracts with processors to ensure there are appropriate provisions in relation to the processor's 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 processors now have direct legal obligations and given that controllers and processors will have the same obligations in areas such as security. Processors are directly liable for certain breaches under the UK GDPR and so may consider seeking indemnities from controllers in relation to data protection fines caused by the controllers.

9. Territorial scope

The UK GDPR applies to all businesses processing personal data in the context of an establishment in the UK. The GDPR has the same effect in relation to establishments in the EU.

Both the GDPR and UK GDPR also apply to businesses outside of the EU/UK in certain circumstances. If a business controls or processes personal data relating to data subjects within the EU/UK, and that processing relates to the offering of goods or services to data subjects based in the EU/UK or the monitoring of data subjects' behaviour in the EU/UK, the GDPR/UK GDPR will apply. Please note that this does not mean that the UK GDPR always applies to UK citizens; it will not apply to UK citizens based outside of the UK.

Non-UK resident businesses that process data relating to UK residents must appoint a representative within the relevant member state, and under the UK GDPR, non-UK resident businesses that process personal data relating to UK residents must appoint a UK representative.

If you would like further information on the issues covered 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.

Katie Hewson
Partner (CIPP/E accredited)

T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Naomi Leach
Partner

T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Ben Sigler
Partner

T: +44 20 7809 2919
E: ben.sigler@shlegal.com

Chloe Haywood
Senior associate

T: +44 20 7809 2348
E: chloe.haywood@shlegal.com

Alison Llewellyn
Senior associate

T: +44 20 7809 2278
E: alison.llewellyn@shlegal.com

Kate Ackland
Associate

T: +44 20 7081 4174
E: kate.ackland@shlegal.com

Bobbie Bickerton
Associate

T: +44 20 7809 2140
E: bobbie.bickerton@shlegal.com

Olivia Fraser
Associate

T: +44 20 7809 2844
E: olivia.fraser@shlegal.com

BD1252-The UK GDPR- an overview-1021