Joelson

GDPR CHECKLIST

Are you ready?

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018.

The GDPR represents a significant updating of the current data protection regime throughout the EU. Although the UK is scheduled to leave the EU in 2019 (as at the time of printing) the GDPR – or a new UK equivalent – will continue to apply to businesses who collect personal data within the UK and the EU.

This guide is intended as a starting point to help organisations – both large and small –prepare for the GDPR, identifying areas where business practices will need to be updated or changed, ensuring that you are ready and compliant come 25 May.

Be aware

Just reading this is a good start.

If you operate a business in the UK you are more than likely to be caught by the GDPR and so you need to know what is changing and what you need to do.

Be sure that all of the key decision makers and stakeholders in your organisation are aware that the GDPR is coming. This is not an "IT issue", it requires co-operation across your business. Depending upon the nature and size of your business, the GDPR could have substantial resource implications.

Leaving things to the last minute is unlikely to be a successful strategy.

Audit your data

What data do you hold? Do you really need to hold it? What do you hold it for? Do you process sensitive personal data, or genetic, or biometric data? Do you share those data with third parties?

These are the kind of questions that will help you identify the areas where the GDPR will have an impact. Carrying out a data impact assessment is a very useful starting point.

Update your privacy notices

The requirements of privacy notices are changing and you will need to review and probably update them. You may need to change how you structure them and how they appear to your customers.

Know the rights of the individuals you deal with

The rights of individuals – the data subjects – are changing, with some significant enhancements coming into force.

For example, data subjects will have additional rights regarding access to the data you hold about them, the right to withdraw their consent to your processing of their data, and the right to object to your processing of their data. You will need to understand how these new rights will impact on your organisation. You may want to put appropriate processes and procedures in place to ensure you respond to the exercise of these rights appropriately.

Be prepared for an access request

As mentioned above, data subjects have the right to access the data you process about them.

The rules about these are changing – for example, you will, in general, no longer be able to charge a fee for responding to a request, and you will need to respond within a month (rather than the current 40 days).

Demonstrate your compliance

One of the biggest changes is that, more than just complying with GDPR, you will need to be able to demonstrate that you are compliant with the GDPR.

This will mean ensuring that you have appropriate processes and procedures in place to make a record of the processing you are carrying out (including, for example, the lawful basis upon which you are relying to process such data).

Be sure that you have lawful grounds to process data

Under the GDPR, you may only process personal data if you satisfy one of the six lawful grounds for doing so.

You may not have considered this before but under the GDPR, there are different implications depending upon which lawful basis you are relying (for example, a data subject can withdraw their consent to you processing their data). You will need to give thought to what basis you are relying on and then ensure that your privacy notices are updated to reflect this.

Refresh your consents

The rules on obtaining consent under the GDPR are more onerous than under the current regime. In particular, consent must be freely given, specific, informed and unambiguous, and there must be a positive opt-in.

If you currently process data on the basis of the data subject's consent, you will need to consider whether that consent will remain valid under the GDPR. It may well need to be refreshed and you will need to consider how this can be achieved before GDPR comes into force.

There are also different rules which apply to using data for marketing purposes and you need to be aware of these changes to ensure that your marketing activities remain compliant.

Think carefully about children's data

There are specific and restrictive rules when it comes to processing personal data about children.

This may be relevant to online entertainment and games developers. You should carefully review the data you process if you think that it may include data relating to children.

Know about privacy by design

The GDPR brings in a new binding concept of "privacy by design", making this the default standard that organisations must adopt.

You will need to consider data security from the outset when processing personal data. Review you data security procedures and data breach procedures and consider updating these where appropriate.

Be ready to report a breach

Ensure that you have appropriate procedures in place to detect, report and investigate breaches because the rules on how and when you must notify data breaches, both to the ICO and the data subjects, are tightening.

A notification needs to be made to the ICO in most circumstances within 72 hours. 72 hours is a very short period of time. You need to have procedures in place, backed-up with appropriate training of staff, to ensure everyone in your team knows what to do when a breach becomes apparent.

Appoint a data protection officer

You need to consider whether you need to appoint a data protection officer or not.

Generally, this will apply to large organisations or those with complex data processing operations, but if you don't have to appoint one, you may consider appointing a "go to" person, especially for the first few months whilst your processes and policies are changing.

Your international business

The GDPR will apply to organisations outside the EU which process the data of EU citizens. There are also specific rules about the transfer of data outside the EU. You will need to consider if these are relevant to your organisation.

What if it all goes wrong?

Last but not least, bear in mind that the penalties for breach of the GDPR can be much higher than under the current data protection regime – as high as €20m or 4% of global turnover! It is very important to get things right.

What happens next?

The ICO is continuously releasing new guidance in relation to the GDPR and updating the information on its website (www.ico.org.uk). It is a great source of information, especially for small and medium sized businesses.

However, we recognise that you may need tailored advice which is specific to your business and your requirements. Our GDPR team can help you with your preparation. In particular, we can:

- Guide you through your data impact assessment
- Advise on your accountability and governance obligations
- Provide further information in relation to Data Protection Officers
- Assist with your understanding of the responsibilities of data processors
- Help you with refreshing consents to process data
- Provide training and template policies on reporting a data breach
- Advise on individuals' rights under GDPR, including your employees' rights
- Update your privacy policies and notices
- Review and update your terms and conditions and contracts

Contact us

If you require further advice please do not hesitate to contact us.

Corporate

Philippa Sturt
Partner
philippa.s@joelsonlaw.com

Philippe Hails-Smith
Partner
phil@joelsonlaw.com

Matthew Overton
Senior Associate
matthew.o@joelsonlaw.com

Employment

David Greenhalgh
Partner
david@joelsonlaw.com

Reema Jethwa
Associate
reema.j@joelsonlaw.com