Blue Saffron
more than just IT

The GDPR at a glance, and a “to do” list to help you prepare for it

The General Data Protection Regulation (GDPR) promises the biggest shake up to European privacy laws for 20 years. It will apply in all European Member States from 25 May 2018.

The GDPR will not only bring a step change in sanctions, with fines of up to 4% of annual worldwide turnover or €20 million, but will also change the way your customers and others expect you to handle their personal information.

Businesses based in the UK should continue to prepare for the GDPR, notwithstanding Brexit. It is likely that the rules in the GDPR will still be applied to the UK for the short to medium term. Moreover, if your business deals with individuals in the rest of EU, you will be caught by the extra-territorial provisions in the GDPR. Similarly, if parts of your business are established in the rest of the EU, those establishments will be directly subject to the GDPR.

This leaflet summarises the key changes under the GDPR, as well as offering a “to do” list to help you prepare for 2018. The changes needed to comply with the GDPR are significant, and you should start to prepare for them now.

We have compiled reosurces that explore this issue in more detail.

More information available at managedit.bluesaffron.com/?s=gdpr

Blue Saffron
more than just IT

Contact Us

Tel: 0844 5600202
Tel: sales@bluesaffron.com

At a glance: what you need to know, what you need to do

Blue Saffron
more than just IT

Area	Countdown to 2018	Extra-territorial reach	Core rules remain the same	Consent	Data subjects' rights	Accountability	Privacy notices	Data protection officers	Data security	Processors	Transfers outside the Union	Sanctions
Summary of Regulation	> The GDPR will apply in all Member States from 25 May 2018. > Businesses that carry out crossborder processing should be primarily subject to the regulator in the jurisdiction in which they have their main establishment.	> The GDPR primarily applies to businesses established in the EU. > It will also apply to businesses based outside the EU that offer goods and services to, or monitor individuals in, the EU.	> The GDPR retains the same core rules as the existing Data Protection Directive but there are some significant changes to those rules. > The concept of sensitive personal data has been retained and expanded to include genetic and biometric data. Using information about criminal offences will also be harder to justify.	> It will be much harder for you to obtain a valid consent under the GDPR. Individuals can also withdraw consent at any time. > Consent to process sensitive personal data or to transfer personal data outside the EU must be explicit. > However, you will not always need consent. There are other justifications.	> There are also potentially significant new rights for individuals, including the "right to be forgotten" and the right to data portability. > The new rights are complex and it is not clear how they will operate in practice.	> Under the GDPR, you must not only comply but also be able to demonstrate you comply. > If you are carrying out "high risk" processing, you must carry out a privacy impact assessment and, in some cases, consult your regulator. This could have significant timing implications for your project.	> The GDPR increases the amount of information you need to include in your privacy notices. > Those notices must also be concise and intelligible.	> You may be obliged to appoint a data protection officer. > The data protection officer must be involved in all data protection issues and must report directly to the highest level of management within your organisation.	> You must keep personal data secure. This obligation is expressed in general terms but does indicate that some enhanced measures, such as encryption, may be needed. > You may have to report security breaches to the regulator and, in some cases, to individuals.	> You will need to include new obligations in contracts with your data processors. > Some aspects of the GDPR are directly applicable to processors. This will be a major change for some suppliers who were previously not subject to data protection law.	> The GDPR prohibits the transfer of personal data outside the EU, unless certain conditions are met. These conditions are broadly the same as those under the existing Data Protection Directive. > Full compliance with these rules will continue to be difficult and requests from foreign regulators will be challenging.	> There is a step change in sanctions. Regulators will be able to issue fines of up to 4% of annual worldwide turnover or €20 million. > Individuals can sue you for compensation to recover both material damage and non-material damage (e.g. distress).
"To do" list	☑ Work out where your main establishment is and who your lead regulator will be. ☑ Keep track of guidance issued by regulators and the European Data Protection Board.	☑ Evaluate if your business (if established outside the EU) is nonetheless caught by the GDPR. If you are caught, you may need to appoint an EU representative. ☑ Consider if you want to take steps to avoid being subject to the GDPR.	☑ Review your existing compliance. ☑ Work out if you are processing genetic or biometric information or information about criminal offences. If so, bring that processing into line with the new requirements of the GDPR.	☑ Review your existing processes to obtain consent to determine if they are valid under the GDPR. ☑ Consider if you can rely on an alternative basis for processing, especially in light of the right to withdraw consent.	☑ Consider if individuals are likely to exercise their new rights against you and what they mean for your business in practice. ☑ Based on that analysis, set up processes to capture, record and act on those requests.	☑ You will need to create and maintain a record of the processing you are carrying out (unless exempt). ☑ You should adapt your product development processes to include a privacy impact assessment.	☑ You will have to update your existing privacy notices. ☑ You should use the most effective way to inform individuals of your processing, such as layered or just-in-time notices.	☑ Work out if you need to appoint a data protection officer or want to appoint one on a voluntary basis. ☑ Consider if you want to appoint a single data protection officer for the whole of your business.	☑ Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate. ☑ Review and update your security measures in light of the increased security obligations in the GDPR.	☑ If you are a controller, update your contracts with processors to reflect the new contract requirements. ☑ If you are a processor, consider the implications of becoming directly subject to the GDPR.	☑ Review your current transfers and consider if they are justified now and will continue to be justified under the GDPR. ☑ You should consider implementing a "structural" transfer solution (such as Binding corporate rules or an intragroup agreement) to justify your transfers.	☑ Review your current level of compliance and bring it up to the level required under the GDPR. ☑ Consider your overall attitude to risk and consider creating a risk assessment framework.

Further information on all these issues is available in our **resources section**
managedit.bluesaffron.com/?s=gdpr