Ten tips for being GDPR compliant

By now, you are likely to have heard about the "GDPR" - the new European data protection law which comes into force on 25 May 2018. Its headlines are: increased data subjects rights, more prescriptive obligations on organisations that process personal data and significant new levels of fines of up to €20 million or 4% of annual worldwide turnover. This new risk profile means that data protection should be a priority for your firm. Below we have set out our top 10 tips to becoming GDPR compliant.

1. Understand your data flows

The first step of any GDPR compliance project should be to undertake a data mapping audit. This will help you identify the data flows within your organisation and understand exactly what personal data you hold, where you get it from, what you use it for and who it is being shared with.

2. Risk rate

Following your data mapping audit, review and assess your current data protection practices and processing activities against the requirements of the GDPR.

Identify any gaps in compliance and risk-rate the actions you need to take by prioritising the activities which present the biggest risk.

3. Review fair processing notices

The GDPR requires that fair processing notices contain much more detail than ever before. This includes information about international transfers and the legal grounds relied on for each use of personal data. This needs to be balanced against the requirement for notices to be transparent, concise and easily accessible and use clear and plain language!

You might want to divide your notice into different sections for different categories of data subjects so that the individual only needs to click on the section that is relevant to him or her. The ICO still recommends using a "layered" approach with the short form 'first layer' inserted in contracts/policy documentation and the long form version hosted on your website.

4. Data security

Deficiencies in data security practices are still by far the biggest cause of ICO enforcement action. Ensure that you have appropriate technical and organisational security measures in place, for example: encryption, pseudonymisation, data loss prevention software, the ability to quickly restore availability and access to personal data, appropriate access controls and a clear desk policy.

Implement processes for regularly reviewing and testing your security systems to ensure the ongoing security of any data processing. Remember non-compliance with your security obligations could lead to heavy fines and significant reputational damage!

5. Review third party contracts and arrangements

The GDPR includes a prescriptive list of requirements that must be included in a contract with a data processor. You should update your template contract clauses and use these in all new engagements. You should also carry out a review of existing third party contracts and vary them where required.

6. Demonstrate accountability with the GDPR

This is a new principle which requires data controllers to demonstrate compliance through written policies and procedures. These must be provided to the ICO on request. Key policies which you should have in place include data security, breach notification, data retention and dealing with data subject request. You will also need to maintain a record of your processing activities which details, amongst other things, the categories of data subject, what personal data you process and the purposes of such processing.

7. Review data retention practices

Review data retention practices to ensure that you are not keeping personal data for longer than is necessary. The more personal data that is held, the more there is to lose or to be stolen. Implement a data retention policy, setting out which categories of data you hold, for how long and why, which could be provided to the ICO on request. Where possible, anonymise personal data.

8. Ensure that you are in a position to comply with data subject rights

The GDPR provides individuals with rights over and above those provided under existing data protection laws. New rights have been introduced including the right to data portability which gives individuals the right to require their data to be transferred to a third party. Ensure that your IT systems have the capability to search and filter information by particular individual and implement an internal data subject rights policy setting out how to deal with and recognise such requests.

9. Create a culture of GDPR compliance and raise data protection awareness

Data protection awareness should be embedded throughout your organisation. A clear governance structure should be implemented reflecting the importance of data protection compliance and ensuring that any concerns or issues can be escalated quickly where necessary. To improve GDPR awareness, ensure that all staff receive training (in particular, bespoke training for roles which handle large volumes of personal data) and know where to access internal data protection policies and procedures.

10. Implement breach response procedures

The GDPR has introduced mandatory breach reporting both to the ICO and data subjects, in certain circumstances. You should implement an internal breach response plan, setting out reporting lines and the procedure for convening and managing a breach response team in the event of a data breach. This should be regularly tested using mock data breach rehearsals.

Contact us

Rhiannon Webster
Partner
Tel: +44 (0) 20 7894 6577
rwebster@dacbeachcroft.com

Jade Kowalski
Senior Associate
Tel: +44 (0) 20 7894 6744
jkowalski@dacbeachcroft.com