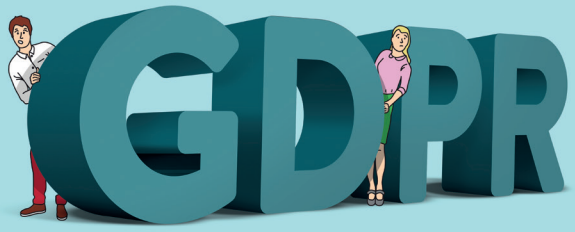
8 Steps to  Compliance

Are you hiding behind it?

1 Consent

How are you seeking, obtaining and recording consent?

You must be able to demonstrate that consent has been freely given and is specific, informed and unambiguous. It must be given on an 'opt-in' basis. You may need to update existing consents now if they do not comply. Special rules will apply to obtaining consent for processing children's personal data.

2 Communication

Are your privacy notices GDPR compliant?

In addition to the current information you are required to give when you collect personal data, you will need to set out your legal basis for data processing and your data retention periods, as well as advise individuals that in addition to other rights, they have a right to complain to the ICO. This information must be communicated clearly and concisely.

3 Holding and Processing Data

What information do you hold and what is your legal basis for processing it?

Under the GDPR you are required to maintain records of your processing activities. You may need to carry out an information audit to ascertain what information you hold, where it came from, what you do with it and who you share it with.

4 Rights of Individuals

Do your procedures comply with individuals' new rights under the GDPR?

Individuals will have greater rights in relation to their data under the GDPR, including rights of access and data portability, to have inaccuracies corrected, to have information erased, to prevent direct marketing and to prevent automated decision-making and profiling.

5 Subject Access Requests (SARs)

How will you comply with the new rules on SARs?

You will now have just a month to comply with a subject access request and will only be able to refuse or charge for requests if they are manifestly unfounded or excessive. Consider what systems you may need to implement to meet the challenge of having to deal with requests more quickly.

6 Data Protection Impact Assessments (DPIAs)

Do you have a strategy for dealing with the new DPIA requirements?

DPIAs will become mandatory in some cases, e.g. where new technology is deployed, where profiling is likely to significantly affect individuals or where processing is large-scale and involves special categories of data. Where a DPIA identifies high-risk processing, you will need to consult the ICO. Take steps now to identify how DPIAs will be carried out and by whom.

7 Data Breaches

Do you know what to do if you detect a data breach?

Make sure you have procedures in place to detect, report and investigate a personal data breach. The GDPR will require you to notify the ICO of certain types of data breach and, in serious cases, the individual affected.

8 International

Do you carry out cross-border data processing within the EU?

If so, map out where your organisation makes its most significant decisions about data processing to determine who your lead data protection supervisory authority is and document it.

Visit www.hcrlaw.com/GDPR