The team

Robert Cobley, Partner

01905 744 806 | 07791 894 955 | rcobley@hcrlaw.com

Rob's specialist practice includes all aspects of IT law and intellectual property, including IP commercialisation, protection and enforcement. Rob regularly advises clients on protecting and licensing their innovative technology and the complex commercial agreements relating to their use.

Steve Murray, Senior Associate

01242 246 494 | 07921 498 467 | smurray@hcrlaw.com

A litigator since qualification, Steve has an innate skill for contentious issues and works with a range of clients from large insurance companies to smaller businesses and private individuals. His specialism is in Intellectual Property issues such as copyright and trade mark infringements and domain name disputes.

Rachael King, Associate Solicitor

01905 746 466 | 07715 060 345 | rking@hcrlaw.com

Having worked extensively in-house as well as in private practice, Rachael has a broad range of experience in commercial work, having acted for insurance companies, PLCs, financial institutions as well as clients in the technology, education and care sectors.

Summary

This quick reference guide has been produced to highlight the key issues arising under the General Data Protection Regulation (GDPR) and to assist organisations in preparing for the effective date of the GDPR, 25 May 2018.

This document is not intended to be an exhaustive statement of the law and gives general information only on the key principles of the GDPR. It is not a substitute for legal advice and we do not accept liability to anyone who does rely on its contents.

For further advice and assistance relating to compliance with the GDPR contact:

Robert Capper,
Head of Commercial Department and Advanced Manufacturing Sector

01905 744814 | rcapper@hcrlaw.com

Are you hiding behind it?

INVESTORS IN PEOPLE | Lexcel Practice Management Standard Law Society Accredited | The Legal 500 United Kingdom | CHAMBERS AND PARTNERS

Quick reference to **General Data Protection Regulations (GDPR)**

Talk to us: 01905 612001

Website: www.hcrlaw.com

Join the discussion: @HCRlaw

A PASSION FOR PEOPLE

harrison clark rickerbys SOLICITORS

COMV156017A

Countdown to 2018

The General Data Protection Regulation (GDPR) will introduce a single framework for the protection of personal data that will apply across all EU member states from 25 May 2018.

Under the GDPR, organisations will face enhanced duties and greater sanctions for breach of their data protection obligations.

Accordingly, organisations should take action now to ensure they are fully compliant with the principles of the GDPR.

The GDPR will introduce new concepts and approaches for the protection of personal data. The good news for organisations is that many of the new requirements under the GDPR are similar to existing core concepts under the Data Protection Act 1998.

Organisations should be aware that the GDPR is still likely to require significant changes to existing processes. Ensuring compliance will take time and it is therefore essential for organisations to plan ahead.

Expanded Territorial Reach

The location of the data subject and not the organisation will determine whether or not the GDPR applies to organisations that do not have an establishment within the EU.

This means that many non-EU organisations will be required to comply with the GDPR even if they were not previously required to comply with the Data Protection Directive.

Consent

Consent must be freely given, specific, informed and unambiguous. It must be a clear indication of the data subject's agreement to the processing of their personal data. Consent has to be given on an opt-in basis and the data subject must have the right to withdraw their consent at any time.

Existing practices for obtaining consent will need to be reviewed and amended to meet GDPR standards. Consider refreshing existing consents where they do not meet these standards.

Rights of Data Subjects

The rights of data subjects under the GDPR are enhanced and, as a result, organisations should carefully ensure that these rights are appropriately addressed.

Data subjects will have the right to be forgotten, data portability rights, the right to have inaccuracies corrected and the right not to be subject to automated decision-making, including profiling.

There are also new rules in relation to subject access requests, including changes to the response time which will be just one month.

Accountability

The GDPR adopts a risk-based approach and requires data controllers to implement appropriate measures to ensure and demonstrate compliance with the GDPR.

Data Protection Impact Assessments are required to be carried out prior to the use of new technologies that are likely to result in a high risk to data subjects.

Any measures identified must be monitored and updated.

Privacy Notices

The GDPR increases the amount of information organisations need to include in privacy notices, such as notification of the expanded rights of data subjects.

Organisations should therefore review existing privacy notices and ensure that any necessary changes are implemented prior to the GDPR coming into force.

These notices and any communications to data subjects must be clear, concise and intelligible.

Data Protection Officers

A senior member of your organisation should take overall responsibility for GDPR compliance. Organisations should also consider whether they are obliged to appoint a Data Protection Officer who has the knowledge and authority to monitor compliance effectively.

As the changes under the GDPR are comprehensive and far-reaching, all members of your organisation should be trained on the GDPR requirements.

Data Security

Organisations must ensure that personal data is kept secure at all times. In some cases, enhanced measures such as encryption will be necessary.

The GDPR requires mandatory reporting of security breaches to the regulator and in serious cases to the data subject.

Organisations should put in place processes to deal with breaches in accordance with the GDPR.

Processors

The GDPR imposes duties directly on data processors in addition to data controllers. The GDPR will impose sanctions for breach on both data processors and data controllers.

Data controllers should identify contracts with data processors and ensure they reflect the GDPR. Data processors should review existing arrangements to ensure these meet their updated compliance requirements.

Transfer out of EU

The GDPR allows the transfer of data outside of the EU only when certain safeguarding criteria are met. A broader range of mechanisms to transfer personal data out of the EU has also been introduced, including approved codes of conduct and certification processes.

Organisations should review their procedures to check whether they are adequate under the GDPR and consider whether new documentation is required, such as binding corporate rules.

Sanctions

The GDPR will significantly increase the maximum fines for non-compliance and regulators will be able to impose fines on data controllers and data processors. The maximum level of fine is €20 million or 4% of total worldwide annual turnover (whichever is greater).

In addition to financial sanctions, there will also be significant reputational damage to organisations if they fail to adequately comply with the GDPR.