PENNINGTONS
MANCHES
COOPER

DATA PROTECTION COMPLIANCE SERVICE

EXECUTIVE SUMMARY

The UK GDPR

Since Brexit, businesses and other organisations that collect and use personal data in the UK need to comply with an adapted version of the EU General Data Protection Regulation (GDPR), plus the Data Protection Act 2018. The UK GDPR broadly mirrors the EU GDPR.

The UK GDPR therefore sets out what organisations must do when collecting, storing, and using personal data. It applies not only to organisations based in the UK but also organisations in other countries, if they offer goods or services to individuals located in the UK or monitor UK residents' behaviour. In addition, if such organisations do not have a business presence in the UK, they will need to appoint a representative in the UK to deal with any queries relating to data breaches or subject access requests.

The EU GDPR continues to apply to UK (and other) organisations that have an establishment in the EU, offer goods or services to individuals located in the EU or monitor EU residents' behaviour. Such organisations need to comply with both the UK GDPR and the EU GDPR. If they do not have a business presence in the EU, they will need to appoint a representative in the EU to deal with any queries from individuals there.

What it means

Like the GDPR, the requirements of the UK GDPR are far reaching. There is an emphasis on transparency and security when processing personal data, as well as individuals' rights and mandatory notification requirements for certain data breaches. The obligation to be accountable requires organisations to put in place comprehensive policies and practices, as well as having organised record keeping. Key obligations such as "the right to be forgotten" and "privacy by design" impact upon how businesses interact with their customers.

Non-compliance presents not only reputational but also financial risk. Breaches are punishable by very significant fines of up to £17.5 million or 4% of global annual turnover (whichever is higher).

The Solution: Data Protection Compliance Service

We are pleased to offer our Data Protection Compliance Service. It's a packaged, end-to-end legal service, designed to enable businesses to achieve UK GDPR compliance. It consists of two key phases. The first phase is delivered at a fixed price and we also have a fixed-fee pricing model for defined scopes of work throughout the process.

It has been developed by us in response to demand from clients, who need a fast and cost-effective solution to data protection compliance.

Further details of the issues arising from the UK GDPR are set out in the pages below, together with additional information on our Data Protection Compliance Service.

ABOUT US

Penningtons Manches Cooper LLP is a leading UK and international law firm with 139 partners and more than 870 staff in total. We have UK offices in the City of London, Basingstoke, Birmingham, Cambridge, Guildford, Oxford and Reading. We also have offices in Singapore, Piraeus, Madrid, Paris and a representative presence in Sao Paulo.

We provide a full range of legal services, with specialist groups in (amongst other areas) intellectual property, technology, commercial, corporate, finance, real estate, shipping and litigation.

We also have excellent international connections with law firms around the world and are a founding member of Multilaw, a top-10 global legal network with over 8,500 lawyers in 70 countries. We are very active within the Multilaw network, with one of our partners having served as chair of the Multilaw Privacy & Information Security group for a number of years.

Our data protection and privacy team

Our highly respected data protection and privacy team is comprised of lawyers drawn from our IP, IT & commercial, employment and commercial dispute resolution teams.

Our team, including seven partners and nine other lawyers, has a wealth of experience in all aspects of UK data protection and privacy laws, including data security, cross border transfers, consent issues, data controller / processor issues, e-mail marketing and social media campaigns, and subject access requests. Our partner Joanne Vengadesan has been recognised as a Global Thought Leader on Data for the UK in Who's Who Legal for 2019 – 2022. She co-chaired the Data Protection group of global technology law association iTechLaw from 2017 to 2020.

We draft and advise on privacy policies, data collection processes, data management policies, data sharing agreements and advise on international data transfers, including the impact of *Schrems II* and carrying out Transfer Impact Assessments. Members of our team also offer expertise in freedom of information laws and the privacy rights of individuals, including applying for and defending privacy injunctions. We advise on data breaches, including assisting clients with reporting to the ICO and helping with breach mitigation strategies.

Our clients include international, listed and private corporations, charities, professional services firms, educational institutions and individuals.

Clients of Penningtons Manches Cooper highlight the firm's responsiveness, value for money and clear advice that is distilled to salient points.

The team is well organised and partners are always available and responsive.

Not only do the firm members have superior technical and legal skills, they offer strategic and practical advice taking into account the business interests of the client. The advice is comprehensive and direct.
The Legal 500

DATA PROTECTION COMPLIANCE: THE CHALLENGES

The background

When the GDPR came into force in May 2018 it was the first major piece of data privacy legislation in the EU for 20 years. The digital world had changed beyond recognition in that time. In the age of cloud-based services, data flows across borders and takes many forms (many of which are unstructured). The quantity of data is growing almost exponentially. Against this background, the EU Commission was determined to introduce a much stronger and more coherent data protection framework. Post Brexit, the processing of personal data in the UK is governed by the UK GDPR, which broadly mirrors the EU GDPR.

Key principles

The key principles of data protection are largely unchanged. Personal data (that is data relating to an identifiable person):

- must be collected, processed, shared and used lawfully, fairly and transparently;
- can only be collected and used for explicitly stated purposes;
- must be relevant and needed for that purpose;
- must be accurate and up to date;
- cannot be kept longer than necessary; and
- must be kept securely.

There are enhanced obligations for certain "special" categories of personal data, namely data relating to an individual's race or ethnicity, politics, religion or philosophical beliefs, trade union membership, genetic or biometric data, health data, and data relating to sex life or sexual orientation.

Transparency

The transparency principle means that privacy policies need to contain detailed information, as specified in the UK GDPR.

Obtaining consent

Pre-GDPR, businesses tended to ensure that data is fairly processed by obtaining consent from the relevant individual. However, consent is not always the most appropriate basis for the processing, and it is now much harder to obtain valid consent.

Under the EU and UK GDPR, consent must be freely given, specific, informed and unambiguous, and it must be given by some affirmative action. It must be requested in plain language and be capable of being withdrawn at any time. Separate consent must be obtained for each proposed use of any personal data. In some cases, where there is a fundamentally imbalanced relationship (such as between an employer and its employees), it won't be possible for consent to be freely given at all (although there are limited other grounds available). Records must be kept of consents which have been obtained.

Data protection by design and default

The UK GDPR requires businesses and organisations to implement 'data protection by design and by default'. This means integrating data protection into processing activities and business practices, from the design stage right through the lifecycle. Although the concept has always been part of data protection law, now it is a legal requirement.

Enhanced rights of individuals

Individuals have a number of rights under UK GDPR most notably the right to have access to information held about him or her (known as "subject access requests"). In addition, individuals have the right to object to or restrict processing, the right of erasure (the so-called "right to be forgotten") and the right of data portability. An increased awareness of data protection rights, partly due to media coverage of data breaches and misuse, has led to businesses receiving many more requests.

Data management

Businesses are required to put suitable technical and organisational measures in place to ensure the security of the personal data they process. Personal data must not be retained for longer than is necessary for the purpose for which it was collected. In addition, organisations are required to maintain records of their processing activities so that they can demonstrate their compliance.

Transfers of personal data require additional consideration in most contexts. Contracts with data processors will need to be reviewed, to ensure that certain new mandatory provisions are included (such as obligations on the processor to assist with data breaches and regulatory investigations, and with facilitating data subjects' rights).

Under the UK GDPR, personal data must not be transferred outside the UK unless there is an adequate level of protection for that data. After Brexit, the UK recognised EU/EEA member states as providing an adequate level of protection, and vice versa, so data can continue to flow freely between the UK and the EU/EEA. Organisations that transfer data outside the EU/EEA, to countries not deemed to provide an adequate level of data protection, need to put in place a valid data transfer mechanism (such as standard contractual clauses). New standard contractual clauses have been issued for such transfers.

Governance

UK GDPR requires certain categories of business to appoint a data protection officer and, where particular data processing activities are viewed as being higher risk, businesses will need to carry out Privacy Impact Assessments (PIAs). There are also strict requirements for reporting breaches of data protection law (both to data subjects and to the regulator).

Sanctions

As mentioned above, the UK GDPR imposes significant penalties for non-compliance, with fines of up to 2% of total global annual turnover or £8.7 million (whichever is the higher) for certain categories of breaches, and up to 4% of total global annual turnover or £17.5 million (whichever is the higher) for the most serious infringements.

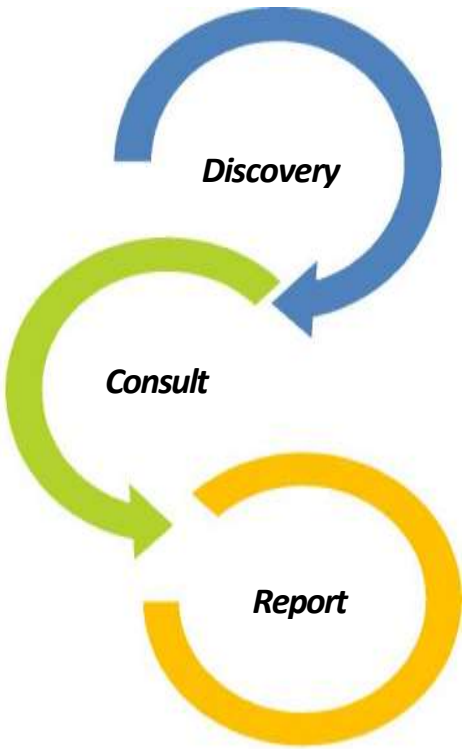
DATA PROTECTION COMPLIANCE SERVICE

How it works

Our Data Protection Compliance Service is designed as an end-to-end solution to enable SME businesses to achieve compliance1[1]. It is a packaged offering, with two phases and a number of modules. The work involved is undertaken by members of our specialist data protection and privacy team, based in the UK.

Phase 1: Discovery

We agree a fixed fee with you for Phase 1: Discovery.



Provision of **detailed questionnaire** concerning data processing activities and collation of key legal documents

↓

Follow up consultation to discuss key issues and request any further information

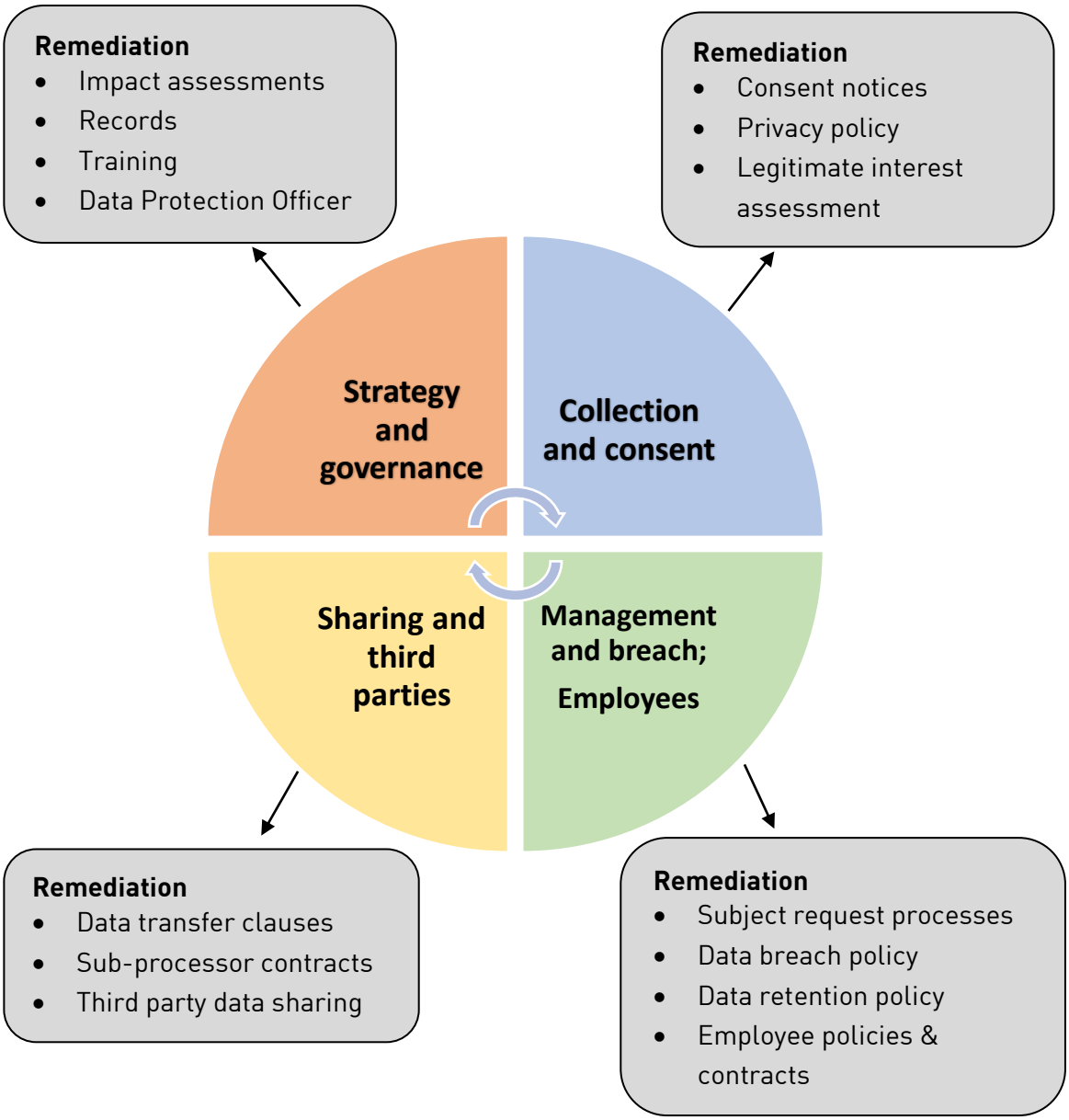
↓

Delivery of red/amber/green (RAG) **analysis report**, outlining key gaps and recommending essential remediation

[1]Our Data Protection Compliance Services is based on UK GDPR and we also advise on EU GDPR. Where our clients need advice on the way the EU GDPR is interpreted and applied in a particular member state, local law advice may be required at an additional cost and we will work closely with our network of lawyers in the relevant EU member states. For certain sorts of business, such as businesses involved in large-scale monitoring, or processing of certain special categories of data or children's data, additional considerations may apply at additional cost.

Phase 2: Remediation

For Phase 2: Remediation, we agree fees with you based on a fixed-fee pricing model.



Remediation activities typically include the following:

Collection and consent

- Updating internal and external data collection policies and procedures.
- Identifying the grounds for lawful processing that are relied upon and confirming that these grounds are still applicable.
- Refreshing consents in line with the requirements of the UK GDPR.
- Maintaining audit trails of such consents.

Management and breach

- Updating breach notification policies and procedures.
- Updating data retention policies.
- Updating data subject policies to cover both subject access requests and other rights (eg request for erasure).
- Updating recruitment documentation, offer letters and employment contracts.
- Implementation policies for employees and internal data processing policies.
- Not included: advice on IT systems security or resilience, or data mapping exercises - these may need to be undertaken by a separate IT consultancy.

Sharing and third parties

- Considering current data transfer mechanisms and whether these are still appropriate. Revisiting data protection clauses in template documents with sub-processors.
- Re-considering the legal basis for cross-border transfers of data with customers and suppliers based overseas.
- Implementing measures to ensure records of processing are regularly updated.

Strategy and governance

- Ensuring that internal governance processes demonstrate compliance.
- Assessing the requirement to appoint a Data Protection Officer and allocate sufficient resource and support for the DPO role.
- Providing training for employees across the business.

KEY CONTACTS

JOANNE VENGADESAN
PARTNER, READING
T: +44 (0)121 312 2601
M: +44 (0)7769 930 490
E: joanne.vengadesan@penningtonslaw.com

ANNA FRANKUM
PARTNER, LONDON
T: +44 (0)20 7457 3205
M: +44 (0)7786 254 053
E: anna.frankum@penningtonslaw.com

HILARY ALDRED
PARTNER, CAMBRIDGE
T: +44 (0)122 346 5465
M: +44 (0)7917 839 324
E: hilary.aldred@penningtonslaw.com

DAFF RICHARDSON
PARTNER, OXFORD
T: +44 (0)1865 581 3647
M: +44 (0)7790 021 452
E: daff.richardson@penningtonslaw.com

GEMMA WOODHOUSE
PARTNER, READING
T: +44 (0)118 402 3842
M: +44 (0)7798 828172
E: gemma.woodhouse@penningtonslaw.com

PENNINGTONS
MANCHES
COOPER

LONDON
BASINGSTOKE
BIRMINGHAM
CAMBRIDGE
GUILDFORD
OXFORD
READING
MADRID
PARIS
PIRAEUS
SINGAPORE

Penningtons Manches Cooper
Incorporating **Thomas Cooper**

www.penningtonslaw.com