Katten

PRIVACY, DATA AND CYBERSECURITY ADVISORY

# Key Data Protection Considerations for Companies Doing Business in the UK/EU

November 5, 2021

The following outlines where Katten can help clients to comply with their General Data Protection Regulation (GDPR) obligations. This note is appropriate for clients that are already doing business in the UK or the EU, or may be considering expanding into, or who offer goods and/or services to individuals located in the UK or the EU.

## What is the GDPR?

The GDPR is a set of EU regulations that came into force in 2018 concerning the processing of personal data. The GDPR introduced onerous obligations on organisations to keep data safe and secure. Failure to comply with the GDPR can result in fines of up to €20 million or 4 percent of a company's total annual worldwide turnover, whichever is higher. The GDPR applies to all organisations located in the EU or UK and those located elsewhere that offer goods and/or services to individuals located within the EU or UK. In practice, this means that the GDPR applies to almost any business that operates in the EU and/or the UK.

Businesses must prove how they comply with the requirements on data collection, storage, use and transfer. If a business cannot demonstrate that it has gone through the process of deciding what personal data it actually needs, mapping its data flows and deciding on its correct legal basis is for processing, amongst other obligations, it may risk investigation by a supervisory authority and ultimately, substantial fines.

Following Brexit, the UK adopted its own GDPR rules (UK GDPR) which mirrors the GDPR. The European Commission has made an adequacy decision in favour of the UK, meaning individuals' personal data belonging to those located in the EU can be freely transferred to the UK without the need for additional safeguards. The UK also recognises the EU as having adequate data protection laws so transfers of personal data belonging to those located in the UK can also be freely transferred to the EU. These decisions will be reviewed every four years.

## Data Protection – Initial Compliance Review

- Companies need to reduce their risk of investigation by a supervisory authority, landing a fine or any claims from affected data subjects. We can carry out a review of a business's data protection policies and procedures to evaluate its compliance and prepare a risk assessment matrix. This may be directly for our clients' businesses to assess current risks of receiving fines with a view to helping clients reduce such risks, or assessing the same from the perspective of a third-party business that our clients may wish to invest in or acquire. We can prepare a compliance checklist with action items for reference.
- Not all businesses will be aware that even if they do not have a UK or EU establishment, the GDPR may still apply if the personal data being processed comes from data subjects who are located in the UK or EU, for example, if goods or services are sold online. We can carry out a data mapping exercise with clients to establish how they may need to comply with the GDPR and work out a plan highlighting the high risk areas to be addressed immediately and the 'nice to have' policies/procedures to be put in place to strengthen compliance.
- **Data mapping exercise** – We can carry out an exercise to identify the data you collect and process as a business including where the data is transferred and for what purpose. Following this exercise we will be able to advise on the various documents and policies the business will need in place to work towards compliance with the GDPR.

- **Privacy policies** – A business will need a privacy policy to notify its customers and website visitors about how it collects, uses and stores personal data through use of its website and to provide goods and services. We can review existing privacy policies, or draft them from scratch to comply with GDPR requirements.
- **Data protection impact assessments (DPIA)** – We can assist with documenting a DPIA, which will measure the effect an organisation's data processing activities has on individuals' personal data, balanced against the rights and freedoms of such individuals. The GDPR requires that organisations conduct a DPIA when their processing could result in a high risk to the rights and freedoms of natural persons.
- **Legitimate interest assessment** – If the business is carrying out direct marketing (i.e., e-marketing to its existing and prospective customer databases), it will be necessary to carry out a legitimate interest assessment and comply with both the GDPR and the Privacy and E-Commerce Regulations. We can help clients with the assessment and provide guidance as to what is needed to comply with the requirements under these laws.
- **CCTV legitimate interest assessment and CCTV policy** – If CCTV is used on-site, whether that be in stores, in warehouses or office spaces, a CCTV legitimate interest assessment will also be required alongside a separate CCTV policy.
- **Data Protection Officer (DPO)** – Under the GDPR, having a DPO is mandatory where an organisation's core activity involves regular, systematic and large-scale monitoring of data subjects, amongst other activities. We can help clients to identify whether they need a DPO and provide background on the DPO role and requirements.
- **Assessing the legality of data transfers** – We can also assess whether clients are transferring personal data correctly, for example, via distribution agreements where customer personal data needs to be transferred to a distributor so their goods can be delivered to the customer. This might also involve a cross-border data transfer, which could require additional safeguards under the GDPR. This may also apply to intra-group personal data transfers. We can work with clients to ensure they do not fall afoul of the GDPR when transferring personal data by ensuring the correct mechanisms are in place to adequately safeguard personal data when it is transferred, either internally within a corporate group, or externally to third parties.
- **Standard Contractual Clauses (SCCs)** – Where a business transfers personal data out of the EU or UK to a third country, it is likely Standard Contractual Clauses are needed to adequately safeguard the cross-border personal data transfer.
- **Processing agreements** – If an organisation has master service agreements in place, we can assist with drafting data processing agreements where there is an element of data processing involved in the contracted services.
- **EU/UK representatives** – Under the UK GDPR, a controller or processor not established in the UK, without an office or branch in the UK, must designate a UK representative where it processes the personal data of individuals located in the UK and either (a) its activities relate to offering goods or services to UK data subjects; or (b) it monitors their behaviour within the UK. Similar criteria for appointing an EU representative applies for non-EU businesses that control/process personal data for individuals located in the EU. We can work with clients to identify whether they need a representative and help to appoint such a representative where needed.

## Websites

- **Website compliance** – If a client's website is accessible in the UK or EU, investors or potential buyers will want to see that it complies with necessary privacy and e-commerce laws.
- **Website privacy and cookies notices** – We can draft GDPR compliant privacy and cookies notices, advise on the appropriate protections needed to inform users of the use of cookies and analytics on the site, as well as help clients to prepare terms of use that complement the online privacy policy.
- **E-commerce regulations guidance** – We are highly skilled at advising on possible e-commerce issues and we can work with clients to ensure their e-commerce marketing procedures are compliant with relevant UK and EU rules, such as direct marketing and unsolicited marketing via email or text.

## Internal/Employment Policies

- We can help to prepare internal management policies to help guide a businesses with their on-going GDPR compliance obligations including:
  - responsibility, roles and reporting obligations;
  - risk assessment/management;
  - consent and revocation;
  - recordkeeping;
  - processor and sub-processor management;
  - standard terms/data processing addendums;
  - data management;
  - data retention;
  - data destruction;
  - privacy by design/default;
  - data protection impact assessments;
  - privacy impact assessments;
  - data transfers;
  - incident response plan and data breach policy;
  - data subject access rights (SARs) requests;
  - employee facing data protection policies; and
  - data protection provisions in employment contracts.

## Ongoing Data Protection Assistance

- We can help prepare and deliver a training programme and a record of training for employees regarding dealing with personal data.
- We can provide a template for recording data breaches, records of consents, revocation and opt-out requests.
- We can provide guidance on SARs if an individual exercises their right of access to their personal data. We will guide clients through the process including responses to SARs and the information they will need to provide in response to the individual making the request.

## CONTACTS

For more information on your data privacy concerns, contact your Katten lawyer or any of the following:


**Christopher Hitchins**
+44 (0) 20 7776 7663
christopher.hitchins@katten.co.uk

**Sarah Simpson**
+44 (0) 20 7770 5238
sarah.simpson@katten.co.uk

**Tegan Miller-McCormack**
+44 (0) 20 7770 5247
tegan.miller-mccormack@katten.co.uk

**Brigitte Weaver**
+44 (0) 20 7770 5235
brigitte.weaver@katten.co.uk

**Emma Williams**
+44 (0) 20 7776 7657
emma.williams@katten.co.uk



Katten katten.com

Paternoster House, 65 St Paul's Churchyard • London EC4M 8AB
+44 (0) 20 7776 7620 tel • +44 (0) 20 7776 7621 fax





11/05/21