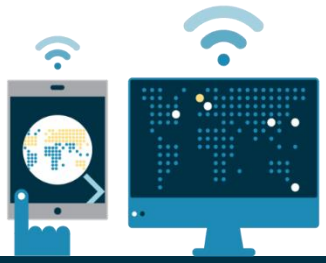
Top 10 Data Protection Tips for US Companies Expanding Internationally



1. Identify personal data you hold

When expanding to the EU or UK, it's important to understand that under the GDPR and UK GDPR, personal data means any information that relates to an identified or identifiable individual (for example, someone may become identifiable when combining to two types of information). This is a very wide definition and there is no complete list of types of personal data but this can include names, email addresses, phone numbers, while also including more obscure types such as location data or IP addresses.

2. Prepare your privacy notices

In the UK and EU your organization is required to be transparent about how your organization manages personal data. As a minimum, most businesses will need a website privacy notice, which tells customers how the company manages personal data and an employee privacy notice, which tells any UK or EU employees how their personal data is held and used. There are requirements about what information needs to be included in a privacy notice, so it's important to ensure that any privacy notice covers these requirements.

3. Get to grips with lawful bases

The GDPR and UK GDPR create a framework that only allows organizations to process – for example, to store, transfer, view, and use personal data if they have a lawful basis to do so. This is the legal reason or legal justification. Under the GDPR and UK GDPR there are six types of lawful basis (listed in Article 6 in the GDPR and UK GDPR). For more sensitive personal or "special category" data, an additional lawful basis is required (listed in Article 2 in the GDPR and UK GDPR). See our full Insight here to get more information.

4. Consider if you need an international data transfer agreement

If you are planning to transfer personal data from your new UK or EU company back to your headquarters, you might need to put in place an international data transfer agreement and additional safeguards. Currently, additional measures are required to transfer personal data from the EU or UK back to the US. These extra safeguards are required even if you are transferring within the same group of companies if the transfer requires taking personal data outside the UK or EU.

5. Check direct marketing rules

There are stringent rules around sending marketing messages in the UK and EU. In general, you cannot send someone a marketing email (where the email address identifies them) unless they have consented. This includes professional and private email addresses. There is sometimes another legal way to send marketing messages but the way to do this varies between each country. Most companies need a solution that allows interested and potential customers to 'opt in' to hear more about their products.

6. Check whether you need to register with a regulator

If your organization is expanding to the UK by forming a company which will handle personal data, the UK company will need to register with the UK Information Commissioner. Failure to register can attract fines. In the EU, the rules on registration vary between each Member State. We recommend checking whether this is a requirement if your business is setting up a company in a Member State.

7. Do you need a data protection officer

If your organization's core activities is around large scale monitoring of individuals, or you process a lot of sensitive or "special category" data, then you might need a data protection officer. Failure to register one when it is required can be a breach of data protection law.

8. Get your records ready

Under the GDPR and UK GDPR you are required to keep records of the type of personal data your organization processes. If you are a controller and you make decisions about how to use the personal data, you need to keep records about the lawful basis your organization is relying on. These records should be detailed enough to include retention periods and provide a useful overview for the business. Making and maintaining these records can be a big task, so its best to start early (upon entering the EU and UK markets).

9. Check your security arrangements

While having good data security practices is always advantageous no matter what jurisdiction you are expanding from (a data leak can always mean logistical worries and bad PR) – in the EU and UK, it could also mean fines. When expanding, it's best to ensure that organization data security practices are in line with current recommendations and they are being implemented throughout the organization.

10. Does your organization have retention periods in place?

It is a requirement under the GDPR and UK GDPR to keep personal data for no longer than necessary for the purpose your organization obtained it. If your organization hasn't already, it will need to consider how to delete personal data that it no longer needs and how this deletion process will be implemented in the future.

Do you have questions? Contact us:

Felix Hilgert
Partner, US

T +1 650 462 4034
felix.hilgert@osborneclarke.com

Emily Barwell
Associate, US

T +1 332 245 4103
emily.barwell@osborneclarke.com