DO YOU WORK CROSS-BORDER OR USE THIRD PARTY SUPPLIERS?

You may risk being in breach of the GDPR and Jersey's data protection law if your data or your client's data is processed outside Europe or within the UK.

We can give you a clear picture of your data location, your risk and advise you on resolving or reducing that risk.

WHAT ARE THE ISSUES?

THE PRIVACY SHIELD

Until recently, a mechanism called the 'Privacy Shield' was considered a sufficient safeguard for data transfer to companies in the US. The Privacy Shield was something US service providers could sign up to in order to agree a set of minimum requirements in terms of processing data to GDPR standards.

In July 2020, as a result of an action by Max Schrems, the Privacy Shield was ruled unlawful. The case is complex but essentially, Schrems successfully argued that U.S. surveillance laws are not compatible with citizens privacy rights under the GDPR. As a result, the Privacy Shield can no longer be relied upon by data controllers.

A 'NO DEAL' BREXIT & DATA TRANSFERS

Currently, the UK has a valid 'adequacy decision' in terms of data but unless a transitional data agreement is reached between the UK Government and the EU before the end of the year, this 'adequacy' may fall away and the UK may be considered 'inadequate' from the 1st Jan 2021.

The States Assembly has agreed to amend Jersey's data protection legislation to allow Jersey and the UK to lawfully exchange information post Brexit but the potential position of the UK as 'third country' in data terms means it remains crucial to be aware of how much of your data is in the UK.

HOW DOES THIS AFFECT MY BUSINESS?

Nearly all companies and businesses use a variety of on and offline sub-processors who may process their data (and their clients' data) in a number of jurisdictions, including the US and the UK. Under data protection legislation, as a data controller (and as a processor), your company has responsibility for this data.

Transferring data to an 'inadequate' jurisdiction (such as the U.S and possibly from January, the UK) may be considered a data protection breach.

The Jersey Regulator has the power to issue fines of up to £300,000 or up to 10% of your annual revenue in a response to a breach.

They can also issue public statements about a company's breach. In addition to fines and action by the regulator, there is the possibility of civil law suits, class actions, reputational damage, plus the costs of remediation to consider.

FOR MORE INFORMATION:

DAMON GREBER
Director, BDO Advisory
+44 (0) 1534 510 100
DGreber@bdo.je

WENDY LAMBERT
Partner, BCR Law
+44 (0) 1534 760 882
Wendy.Lambert@bcrlawjersey.com

www.bdo.je

www.bcrlawjersey.com

BCRLAW

BDO

REGULATORY ADVICE

The Regulator's advice is clear in terms of the Privacy Shield. Consider the extent to which you rely on it. Then either find an alternative method (such as standard contractual clauses provided the receiving jurisdiction provides the same standard of protection for data subjects as is provided in Jersey) or cease data transfer.

In terms of Brexit, if the UK does become an inadequate jurisdiction, the issue would be very similar.

REDUCING YOUR RISK

Many businesses do not have a clear picture of where their data is. Even companies that have mapped their data have not considered the data processed by their service providers, for which they are still liable.

We can give you a clear picture of your data locations, your risk and advise you on resolving or reducing that risk.

Not only will this assist you in reducing your risk, but it will demonstrate to the regulator and your clients that you take the security of your data seriously.

How we can help you

OUR DATA MAPPING & ASSESSMENT PROCESS

1. Map and document the location of your company's data
2. Assess the extent to which you rely on the (now defunct) Privacy Shield
3. Investigate how much data is transferred to and from the UK
4. Review the privacy statements of your third parties
5. Review any data sharing contracts you have entered into with any third parties
6. Determine the volume and nature of data you are responsible for outside of the European Economic Area
7. Advise you about possible remediations and mitigations
8. Provide all of the above in a concise and pragmatic report

www.bdo.je **www.bcrlawjersey.com**