

Client Alert: Munich Court Action Launched Over Privacy Shield

Date : October 14, 2020

Introduction

On 9 October 2020 a German pressure group issued proceedings in Munich in what is possibly the first civil action against a multinational corporation for failure to clarify its data transfer position after the death of Privacy Shield. The case serves as a reminder that organisations need to develop a plan quickly to be able to transfer data out of the EEA.

What was this case about?

The case has been brought by German consumer platform Europäische Gesellschaft für Datenschutz mbH (EuGD) against Amazon. EuGD says that it is bringing the action on behalf of a German Amazon customer. In Germany representative actions by consumer groups are more common than in other parts of Europe.

Amazon is accused of violating GDPR and of 'illegally' transferring data to the USA. EuGD says that Amazon has ignored a request from the plaintiff for details as to any lawful means for transferring the data. It also says that Amazon's privacy policy still refers to Privacy Shield which was struck down by the European Court in July. There is more detail on that ruling here <https://bit.ly/pshielddead>.

Practical tips

In our view every business should work on a data transfer response plan. Even if this is a work in progress it might be something that they can show a potential claimant, a DPA or a court if they are asked questions. It's a strategy which we used after the fall of Safe Harbor and it worked well for many then. The plan might also be something that will reassure customers, employees and other stakeholders. That plan might include:

1. Thinking about how you transfer data. If you rely on Privacy Shield you will need to look at another way – that might be a beefed-up SCC process or so-called Binding Corporate Rules (BCRs) – or in some cases both;
2. It is also important to look at how those you do business with those who have used Privacy Shield to legitimise data transfers too – for example if you have a global HR platform, a global payroll provider, a travel management company or a whistleblowing helpline they may rely on Privacy Shield. You can check to see if they are on the list here: <https://www.privacyshield.gov/list> In some sensitive areas you might want to look at securing service providers in the EEA instead;
3. In a post-GDPR world employees and customers are likely to ask questions about the way in which you make data transfers lawful. Be ready for their questions. Some prepared FAQs may help HR team and contact centres respond to these questions. Works councils are also likely to ask questions too;
4. Look at your transparency obligations. Many organisations specifically refer to Privacy Shield in their privacy policies for example as Amazon allegedly did here. Privacy policies will therefore need a review. You might need to alter other documents too including internal notices to employees and GDPR Article 30 records;
5. It is tempting to think that since the European Court has ruled that SCCs are valid, it's business as usual concerning SCCs. However, as the European Court has indicated, even where a business relies on SCCs, data protection due diligence may still be required in addition. Additionally, it is expected that under GDPR the European Commission will be revising SCCs – so businesses may at some point in the future need to adapt/update their existing SCCs; and,
6. This year, under Brexit, the UK and the EU are trying to hammer out a new relationship for the future. This should include data protection arrangements with a possible adequacy decision for the UK. The UK itself is also expected to introduce new UK data protection legislation – this can be expected to also deal with data transfers, for example we may see UK-specific SCCs and even a UK-US Privacy Shield. So businesses also need to follow these developments..

For other articles that we have written about data protection issues please see here:

<https://www.corderycompliance.com/category/data-protection-privacy/>

For details about Cordery's GDPR Navigator subscription service, which includes short films, straightforward guidance, checklists and regular conference calls to help you comply, please see here: www.bit.ly/gdprnav.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

[Jonathan Armstrong](#), Cordery, Lexis House, 30
Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com



[André Bywater](#), Cordery, Lexis House, 30
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Farringdon



Image courtesy of H&M