European Data Privacy Update

Breaches of Privacy Regulations reach Europe

In January 2012, the European Commission proposed a comprehensive reform of Data Protection rules in the EU. After much discussion and negotiation, the long-awaited EU General Data Protection Regulation (GDPR) is expected to be adopted at the beginning of 2016. Finally, as customers of these data gathering giants we can breathe easy - or can we?

October has certainly been a busy month for cyber criminals in the UK. Customer databases of Marks & Spencer, British Gas, Talk Talk and Vodafone have all been breached. The result of these events is anticipated by companies to be an "avalanche of cyber security regulation in Europe", according to the FT[1]. As a customer of the above household brands you may actually now be more interested at how these companies will be regulated to ensure your private data is better protected.

The aim of the new GDPR is to harmonise the current data protection laws in place across the EU member states. The fact that it is a "regulation" instead of a "directive" means it will be directly applicable to all EU member states without a need for national implementing legislation, although the 2 year implementation framework means it won't be enforceable until 2018.
Businesses want to do right by their consumers as well as by their investors, but these stakeholders may have competing interests when it comes to consumer data. Protecting your privacy is an expensive business, although failing to protect privacy can be more costly – as can been seen in the Weltimmo and Schrems matters recently put before the Court of Justice of the European Union (CJEU).

In Weltimmo, the CJEU is being asked to consider what jurisdiction the Hungarian Data Protection Supervisor might have over a website for Hungarian customers, run and hosted in Slovakia. The ruling could impact the debate over jurisdiction, and may make it easier for local regulators to enforce their laws against companies based in other jurisdictions. Companies may have to answer to or defend themselves against multiple Data Protection Authorities (DPAs).

Schrems concerns a privacy activist, Mr. Max Schrems, who claimed that Facebook wasn't sufficiently protecting users' data (borne from revelations by Edward Snowden, the former NSA contractor, in 2013 that the US intelligence agencies are spying online). As a result, in early October, the CJEU found the EU-US Safe Habor Agreement to be invalid. This is a major blow to the in excess of 4,000 companies which rely on the Safe Harbor Agreement to transfer data between the two continents.

The Safe Habor Invalidation Debacle

The global concern about Intelligence and online activities has also been fuelled recently within Europe, with the UK's recently released draft law; referred to as the "snoopers charter". The draft law proposes to allow UK intelligence agencies access to online material from the last year without the requirement to obtain consent from users.

FT:Businesses braced for bout of regulation on cyber security, 30 October 2015. Available at: http://www.ft.com/cms/s/0/817f4146-7e4e-11e5-a1fe-567b37f80b64.html#axzz3qXTji0fF

Contact Us

If you would like to know more about how we can help you, please do not hesitate to contact us.

LYNDSEY BAUER
Partner
E lbauer@paragonbrokers.com
T +44 (0)20 7280 8228

WILLIAM WRIGHT
Vice President
E wwright@paragonbrokers.com
T +44 (0)20 7280 8252

ERICA CONSTANCE
Vice President
E econstance@paragonbrokers.com
T +44 (0)20 7280 8285

The invalidation of the Safe Harbor Agreement now means that companies have to quickly find a solution to maintain the legality of transferring data across the Atlantic. There are other alternative mechanisms in place, such as standard contractual clauses and Binding Corporate Rules (BCR). However, logically the issues with the Safe Harbor Agreement could be equally applied to these mechanisms, also rendering them invalid.
So, whilst the US Department of Commerce and the European Commission continue negotiations regarding Safe Harbor 2.0 or come to some other solution, we can only wait and see what will be the immediate effect and repercussions to businesses. Does the invalidation of a privacy regulation therefore mean companies are now in violation of the regulation?

It has been suggested by Brian Hengesbaugh of Baker & McKenzie that receiving an enforcement action from a DPA would be a misuse of legal authority with good faith actors. Whilst the majority of DPAs in Europe have advised that they won't be taking any immediate actions, the Spanish DPA, the Agencia Española de Protección de Datos (AEPD), sent a letter to all Safe Harbor certified companies, on November 3rd, providing guidance on alternative protection measures for data transfers. In return, all of those companies that received the letter must report back to the AEPD no later than January 29th, 2016 to advise what alternative mechanisms they have implemented. Whilst Spanish companies now have some clarification on the situation, other companies are still living with the uncertainty of how potential actions from regulators driven by disgruntled individuals will affect them.

How will the Safe Habor invalidation affect insurance?

Breaches of privacy regulations are covered under a cyber insurance policy. However, the question remains, if DPAs take action against Safe Harbor certified companies do insureds have an obligation to notify their insurers? Should cyber insurers should be expecting wide spread losses across their portfolios?

Dan Trueman, Head of the Cyber Division at Lloyd's Syndicate Novae, has expressed concern that all cyber policies in his portfolio may be at risk of having a notification made against them for the breach of the Safe Harbor Agreement. Dan is keen for the regulators to clarify the situation: "The intent is still to cover breaches of privacy regulations and once we are clear on how this will look going forward in regards to transfer of data between the US and EU, the cyber insurance policies can be amended, if required, to continue to provide relevant cover to our clients. We are, obviously, concerned that current policies are likely to not cover effectively or even exclude such issues due the fact that until a clear replacement regime emerges, breaches of regulations could simply be deemed to be wilful."