Contractual approval

upheld the complaint and also named the brand in its adjudication (Club Website Ltd, 8 January 2014)).

It is therefore prudent (and will help advertisers to limit their legal and regulatory compliance risks) for advertisers to enter into contracts with their affiliate marketers that cover this area of compliance. A brand would be wise to have approval rights over all ads created for its benefit or to at least have clear guidelines that all affiliate marketers are compelled to follow.

Anna Williams, associate director, Osborne Clarke, London

Bavarian DPA takes tough line on email encryption

Hendrik Schöttle

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 140–142.
doi:10.1057/dddmp.2014.71

What happened

In September 2014, 750 Bavaria-based companies found a notice letter from the Bavarian Data Protection Authority (DPA) in their mailboxes. After having scanned about 3,500 email servers (mx records) of about 2,200 companies with an automated scanning tool, the authority found that 750 email servers did not comply with current security standards. The authority requested the companies to update their servers accordingly. Now the companies have to react in order to avoid further steps — administrative fines are not excluded.

Automated breach discovery

The Bavarian DPA (Bayerisches Landesamt für Datenschutzaufsicht) had already used automated scanning tools in the past in order to discover data protection law breaches and prosecute the implicated companies. In this case, the DPA took a detailed look at data security and approached companies that had at least one of the following security issues:

- The email server did not offer encrypted connections (STARTTLS for the establishment of an encrypted connection and respective encryption for the following data exchange). *Note:* The DPA does not require end-to-end encryption, which is usually achieved by encrypting the emails themselves, for example by using PGP, GnuPG or a comparable encryption tool. The encryption that the DPA requests only affects the connection between email clients and servers. However, with public wireless hotspots becoming more and more widespread, it has become a common exercise by hackers and script kiddies to read unencrypted email traffic sent over publicly accessible, unencrypted wi-fi

connections, which is prevented by encrypted server connections as requested by the DPA.

- Even when offering encrypted connections, Perfect Forward Secrecy had not been implemented. To date, many encrypted connections use the same encryption keys over time. If a third party records encrypted traffic for a long time and gets hold of the encryption key later on, this party is able to decrypt all encrypted traffic it has recorded in the past. This is what many IT security experts fear happened in the course of the Heartbleed bug (see below). In order to prevent decryption of pre-emptively stored data, Perfect Forward Secrecy demands frequent changes of encryption keys.
- The Heartbleed bug was still present. This has been one of the most severe security vulnerabilities of recent years. Even though information on it has been disseminated in the media, a large number of IT systems are still vulnerable. The Heartbleed bug allows anyone with sufficient technical skills to read data — including emails and private encryption keys — from every affected device via publicly available interfaces. No specific access to any hardware or software is required, just an internet connection. The bug is contained in certain versions of the OpenSSL library, a common tool for implementing encrypted communication, and widely used in all kinds of devices from servers to android smartphones.

Enforcement action

The DPA sent out notices to the companies affected and requested further information about the breach. The concerned companies now have to remedy the security breaches as soon as possible. The DPA highlighted its ability to impose administrative fines in case of non-co-operation and warned that it may instruct the companies to take appropriate measures. The Bavarian DPA announced that it may also provide the scanning tool to DPAs of other German Federal States. And, in fact, the DPA of Baden-Württemberg did scan 11,000 websites for the Heartbleed bug and found 46 vulnerable providers that were approached in the same way.

Why this matters

All email servers affected

Every company in Germany should now ensure its compliance with the requirements outlined above. But in case the Heartbleed bug should still be unfixed, a possible contact from the DPA is not the main problem given the seriousness of the potential data leak. In addition, the foregoing affects almost every company, not only public email providers. If a company receives emails under its own domain name, it is running an email server and has to comply with the requirements above. The DPA highlights that companies that have outsourced their email service are also responsible for their outsourcer's compliance.

Heartbleed fix needed

The foregoing has shown that German DPAs are now proactively scanning IT that is accessible through the internet for security vulnerabilities. In this case, compliance with legal requirements can easily be checked and re-checked after having sent out notices. Thus, it should be in every company's interest to fix at least the Heartbleed bug as soon as possible.

Need for updating

A more general but nonetheless important point that rings true throughout the EU is that unencrypted email servers are definitely no longer state-of-the-art and should be updated. Companies that were approached by the DPA should act as fast as possible in order to avoid administrative fines. But also those companies that have not been contacted by the DPA should take action, including the implementation of Perfect Forward Secrecy. It may be better to plan such implementations in advance, instead of being forced to update the systems in the very short term and under the pressure of possible fines.

Hendrik Schöttle, partner, Osborne Clarke, Munich

ICO publishes draft privacy seal scheme

Sue Gold

Journal of Direct, Data and Digital Marketing Practice (2014) **16**, 142–144.
doi:10.1057/dddmp.2014.72

Who: Information Commissioners Office (ICO)

Where: United Kingdom

When: 3 September 2014

Law stated as at: 9 September 2014

Third-party privacy seals

What happened

The ICO has published draft framework criteria for a scheme whereby third-party privacy seal schemes can obtain the ICO's official endorsement. It has issued a consultation document for comments by 3 October 2014.

The ICO is planning to endorse at least one scheme operated by an independent third party in the United Kingdom for a minimum of 3 years. The consultation invites comments on the framework criteria against which proposals for schemes will be assessed. The ICO will then invite proposals later this year, with a view to selection in early 2015 and launch in 2016. In order to be selected, the scheme operator will need to be accredited by the UK Accreditation Service (UKAS).

Background

The world has changed and both consumers and regulators want to be able to quickly identify where there are good privacy standards — accountability and transparency are key. Although accreditation schemes, particularly for website privacy policies, have been very popular in the United States, their adoption and use in Europe has been slow.

ICO proponent of private schemes

This may be changing and the ICO is a strong proponent of the adoption of 'privacy seals' schemes to indicate that a business operates and