

HAPPY GDPR-VERSARY! HSF REFLECTIONS ON A YEAR OF GDPR REGULATION

24 May 2019 | London
Legal Briefings

The GDPR came into effect almost a year ago on the 25 May 2018. As the most significant reform of data protection law in Europe for over 20 years, the legislation raised expectations of a cultural shift in attitude to data privacy. A year on from the fanfare of implementation, this bulletin looks at key aspects of what we have seen and learnt since implementation, and what we can expect for the future.

ENFORCEMENT

Although we are still waiting for a 'GDPR mega fine', we have seen a EUR 50 million fine levied by the CNIL in France and there have also been some interesting enforcement decisions coming out of Europe in the first 12 months. There have been rumours of a fine matrix being developed by the regulators to help assess the level of fine to be imposed but, for now at least, it remains unclear how fines are calculated and when a 'mega fine' may be appropriate.

Interesting enforcement action to note so far includes:

UK: ICO finds HMRC to be in “significant” breach of data protection legislation but does not impose a fine

In May 2019, the ICO found HMRC in the UK to be in “significant” breach of the GDPR by processing special category biometric data (voice recognition data) without a lawful basis. However, instead of imposing a monetary penalty, the ICO issued an enforcement notice requiring HMRC to delete the relevant data by early June 2019. For more information on this enforcement action, see our blog post [here](#).

Belgium: Court of Appeal asks CJEU for GDPR guidance on the ‘one stop shop’

In May 2019, the Belgian Court of Appeal asked the European Court of Justice for help interpreting the application of the GDPR’s ‘one stop shop’ and whether the designation by companies of a lead supervisory authority in Europe precludes any other European supervisory authority from taking enforcement action against that company. The results of the case will either open or close the doors for regulators across Europe to cast aside the one stop shop when looking to enforce GDPR compliance in their home jurisdiction. For more information on this enforcement action, see our blog post [here](#).

Poland: When is it a disproportionate effort to provide a privacy notice?

In April 2019, the Personal Data Protection Office in Poland issued a €220,000 fine to a digital marketing company for breaching its obligations under Article 14 of the GDPR (i.e. to provide a privacy notice to individuals). The decision has some important practical implications for organisations, including that: (i) the collection of publicly-available information from the internet does not relieve you of your obligations under the GDPR; (ii) a significant cost (in this case €8 million) involved with providing privacy notices to individuals is not sufficient to be able to rely on the ‘disproportionate effort’ exemption under Article 14; and (iii) the GDPR is not prescriptive about how individuals must be provided with privacy information but the ‘passive’ posting of a notice on a website is unlikely to be sufficient where the individuals are unaware of the collection of their data. For more information on this enforcement action, see our blog post [here](#).

Germany: German competition regulator takes enforcement action against Facebook for data issues

In a slight move away from privacy regulation, the German competition authority, the Federal Cartel Office, announced the results of its investigation into Facebook in February 2019. The decision highlights the ever increasing tension between competition and privacy regulation. The FCO found that Facebook had a dominant position in the German market for social networks, and abused this with its data collection policy. The FCO did not impose a fine on Facebook, but has instead required Facebook in the future to only use data from non-Facebook sources where it has users’ voluntary consent, the withholding of which cannot be used to deny access to Facebook. For more information on this enforcement action, please see our blog post [here](#).

UK: First extra-territorial enforcement action commenced by the ICO

In October 2018, the UK data protection regulator, the ICO, issued its first enforcement notice under the GDPR. The notice was particularly noteworthy because it was issued against a company located in Canada, which does not have any presence within the EU. Despite the breaches being alleged, the enforcement notice was the first issued by the ICO relying on the extra-territorial provisions of the GDPR under Article 3. For more information on this enforcement action, please see our blog post [here](#).

GUIDANCE

For many companies, a frustrating aspect of GDPR compliance over the last year has been the uncertainty. One year on from GDPR implementation and many questions remain unanswered. But we have now started to see signs that fundamental questions may eventually be answered and new regulatory guidance is starting to drip feed through the process.

Interesting regulatory guidance published over the last year includes:

A global regulation? EDPB guidelines on GDPR's extra-territoriality provisions

The expansive nature of the GDPR's extra-territoriality provisions has resulted in many organisations outside of Europe questioning whether or not they are subject to the GDPR regime. The market has eagerly awaited any guidance in respect of how Article 3 of the GDPR should be interpreted, and so the [draft EDPB guidance published late last year](#) was welcomed by the data community and the market as whole. However, whilst the draft guidance answered certain questions about the application of the GDPR, it also left a number of gaps and so we are still awaiting the final version of the guidance in the hope that some of those gaps will be closed. For more information on this guidance, see our blog post [here](#).

EDPB guidance on when processing is “*necessary for the performance of a contract*”

In April 2019, the EDPB published guidance on the ability of online service providers to rely on the fact that processing is necessary for the performance of a contract in order to legitimise their processing of personal data. Although aimed specifically at online services, the guidance will nonetheless be useful for all controller organisations looking to rely on this processing condition. The guidance adopts a fairly narrow approach to interpretation with an objective assessment of “necessity” being required as opposed to relying on what is permitted under or required by the terms of a contract. For more information on this guidance, please see our blog post [here](#).

EDPB opinion on the interplay between GDPR and ePrivacy

With companies having completed their GDPR compliance programmes, thoughts are now turning to the next major piece of European regulation in the data privacy sphere, the proposed ePrivacy Regulation, and how ePrivacy interacts with the GDPR, particularly with respect to cookie consent and email marketing. In March 2019, the EDPB published an opinion on the interplay between GDPR and ePrivacy which, whilst interesting, also confirmed that the whole ePrivacy regime is currently being renegotiated at a European level and the new ePrivacy Regulation could further change the position outlined in the opinion. As such, the opinion itself appears to be of minimal use for companies. For more information on this guidance, please see our blog post [here](#).

WHAT'S STILL TO COME?

One year on from GDPR implementation and we've seen limited enforcement action and even less regulatory guidance, meaning that companies are still having to try and find their way through compliance without direction. Much remains unknown and unanswered but what can we expect (or hope) from the next 12 months?

Brexit

The Brexit issue rumbles on without much/any clarity or certainty. We know that an adequacy decision for the UK is extremely unlikely in the short term but whether or not an interim transition deal is achievable (including with respect to data protection and data transfers) remains unknown at this stage.

International transfers

Although the results of the EU-US Privacy Shield annual review in 2018 seem to confirm that the Privacy Shield remains intact for the short term, there remain significant uncertainties around the future of other compliant international data transfer mechanisms. In particular, the validity of the so-called Standard Contractual Clauses ("**SCCs**") continues to be challenged through the courts which could result in the SCCs being struck down by the CJEU in the same way that the US Safe Harbor was in 2015.

Continuing on the theme of international transfers, we are also still awaiting the publication of updated versions of the SCCs. The current versions still refer to the 1995 Directive instead of the GDPR but cannot be amended for sense without the risk of invalidating them. There are rumours that the EU Commission has started to consider an update, including potentially updating the controller to processor SCCs to include Article 28 obligations. However, we have yet to see anything concrete coming out of Europe.

ePrivacy Regulation

As mentioned above, the ePrivacy Directive is currently being renegotiated and was originally intended to be ready in time for the GDPR implementation. However, the failure of the European institutions to agree on a number of issues has resulted in multiple delays and it now does not look likely that a draft will be agreed before the end of 2019/early 2020, meaning that the situation regarding cookie consent and email marketing is likely to remain uncertain for a considerable period of time.

Enforcement

As noted above, we are still awaiting a GDPR 'mega fine' but we also haven't yet seen much in the way of significant volumes of enforcement action in order to be able to gain any meaningful insights into enforcement. There are rumours of significant enforcement actions in the pipeline from the ICO and the Irish Data Protection Commissioner, and we also know that there have been a number of material personal data breaches since implementation of the GDPR, but we will have to wait and see what happens in year two of GDPR.

Individual rights and data disputes

Although the GDPR provided for enhanced data subject rights for individuals, we have also started to see it being used innovatively as a mechanism by individuals to assert other rights, including human rights and the right to privacy. We have seen Prince Harry assert that a news company's photograph of him at home was in breach of GDPR, and a claim against the Police for their use of facial recognition technology has recently started in Wales. Going forward, we are therefore likely to see GDPR used as a tool in disputes. For more information about this, please see our blog post [here](#).

Data breach compensation

Perhaps the elephant in the room sits with data breach compensation. In April 2019 the Supreme Court granted Morrisons permission to appeal against the Court of Appeal ruling that it was vicariously liable for its employee's misuse of data, in the first successful UK class action for a data breach. Whilst the date for the Supreme Court's hearing is still to be confirmed, the appeal is likely to take place during the course of 2020. For more information on the case, please see our blog post [here](#).

New emerging technologies

The age-old issue of technological innovation outpacing the ability of legislation to keep up has reared its head only one year into the GDPR's lifecycle. Organisations are having to apply the text of the GDPR to scenarios including blockchain technology, connected and autonomous vehicles and AI techniques that simply weren't envisaged at the time of writing. In this rapidly evolving technological landscape, the need for regularly updated, up-to-the-minute official guidance in respect of these types of scenarios has never been greater but this will be an extremely challenging demand for the regulators to satisfy.

To keep up to date with the latest legal developments as they happen, please subscribe to our data blog [here](#).

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com



CLAIRE WISEMAN
PROFESSIONAL
SUPPORT LAWYER,
LONDON

+44 20 7466 2267
Claire.Wiseman@hsf.com



LAUREN HUDSON
ASSOCIATE, LONDON

+44 20 7466 2483
lauren.hudson@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2022

SUBSCRIBE TO STAY UP-TO-DATE WITH INSIGHTS, LEGAL UPDATES, EVENTS, AND MORE

Close