GDPR ENFORCEMENT
A CHANGED LANDSCAPE

Bruce Macaulay, Eve-Christie Vermynck, Oscar Tang, Daniel Millard, Aymeric Boëlle and Angus Goalen of Skadden, Arps, Slate, Meagher & Flom review the latest trends in enforcement of the General Data Protection Regulation (*2016/679/EU*).

Central to the expansive rights and obligations provided for under the EU General Data Protection Regulation (*2016/679/EU*) (EU GDPR) and the UK GDPR, the version retained in UK law through operation of the European Union (Withdrawal) Act 2018 (collectively, the GDPR), are the corresponding powers of enforcement that are granted to data protection authorities (DPAs).

Almost three years on from the GDPR coming into force, enforcement is starting to pick up pace and the teeth of the GDPR are beginning to show. From multi-million pound fines imposed on British Airways and Marriott Hotels by the UK Information Commissioner's Office (ICO), to the 128 fines issued by the Spanish DPA in 2020, there has been a clear amplification in the activity of the European and UK DPAs (*see Exclusively online article "ICO fine for BA: iron enforcement with a velvet glove", www.practicallaw.com/w-027-9929*).

This article looks at the latest trends in GDPR enforcement, in particular:

- The increasing attention being paid to cookies and the accompanying enforcement of cookies-related violations.
- An assessment of the "one-stop shop" mechanism through which the GDPR is enforced and the emerging strain that increased enforcement of the GDPR is placing on this mechanism.
- The broader steps being taken by DPAs that are emblematic of the growing trend towards enforcement.

COOKIES ENFORCEMENT

In the early days of the internet, every visit to a website was like the first visit. Websites had no way of remembering who had already visited their pages. In 1994, Lou Montulli helped the internet to remember this information by placing small text files on the devices of website users, allowing websites to track users' browsing history and the amount of time spent on a certain webpage, and save website preferences, such as currency and location. Mr Montulli had invented the cookie.

The use of cookies has shaped the way that the internet works, allowing website operators to perform analytics to measure the success of website content, and, perhaps most significantly, to personalise content depending on users' browsing history. This has spawned industries from data analytics to adtech, with global adtech revenue totalling around $325 billion in 2019. These developments have been made possible through the widespread use of cookies. If personal data are the modern-day oil, cookies are the oil rigs.

Regulation of cookies

As the use of cookies has proliferated, so too has the body of law and regulatory guidance regulating their use. Two legal regimes are of principle importance to cookies regulation within the EEA and the UK: the GDPR and the Privacy and Electronic Communications Directive (*2002/58/EC*) (e-Privacy Directive). The provisions of the e-Privacy Directive, as implemented in the domestic law of each EU member state, take precedence over the more general terms of the GDPR, on the basis of the doctrine that, if two laws apply, the law governing a specific issue applies as against the law governing the issue more generally.

Central to the e-Privacy Directive regime is the principle that a user's consent must be sought and obtained before first-party and third-party non-essential cookies are placed on the user's devices. The request for consent must be accompanied by clear information, in intelligible language, about the purpose for which any cookies are used and for how long these cookies are going to be in place.

As the e-Privacy Directive is silent on the concept of consent, it is judged against the GDPR standard. As such, wherever non-essential cookies are placed on a user's device, the user's consent must be specific, informed, unambiguous and given freely. Once valid consent has been given, it must be as easy to withdraw as it was to give.

DPAs and regulating cookies

To assist organisations with their navigation of the e-Privacy Directive and the GDPR, various DPAs have issued regulatory guidance. For example, in July 2019, the ICO issued guidance clarifying the inter-relationship between the GDPR and the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*) (*see News brief "ICO's cookie recipe: consent is the missing ingredient", www.practicallaw.com/w-021-3574*). The ICO strongly encouraged website owners to carry out cookie audits to assess the compliance of their cookie practice with applicable law and regulatory guidance.

More recently in October 2020, the French data protection authority, Commission nationale de l'informatique et des libertés (CNIL), also issued revised regulatory guidance on cookies including practical steps and guidance for organisations (*www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation*). The CNIL's guidance will be enforceable from April 2021. After the grace period, organisations can expect increased scrutiny from the CNIL over areas modified by its revised guidance, namely:

- The provision of two clear buttons of equal prominence labelled "accept all" and "refuse all".
- That organisations should retain the fact that a particular user has opted out for a certain period of time, with six months suggested as best practice.
- Where a cookie allows the user to be tracked on other websites, the CNIL recommends that consent is obtained on each of the relevant websites to ensure that the user is fully aware of the consequences of providing consent.

The ICO guidance and the CNIL guidance, along with guidance from other DPAs that broadly align with the position of the ICO and the CNIL, add to the increasing body of law and regulatory guidance to which organisations must pay heed when assessing the legality of their own use of cookies.

DPA actions

Since 2019, the CNIL has made targeted advertising, including cookies, an enforcement priority, positioning itself as a leader in the cookie enforcement sphere. Cookies raise clear data protection issues because of their potentially intrusive nature and ubiquity, and the CNIL has observed strong public awareness of online tracking, especially since the implementation of the GDPR.

The CNIL has also received a high volume of complaints focusing on targeted

CNIL enforcement actions

The French data protection authority, Commission nationale de l'informatique et des libertés (CNIL), has taken a number of recent enforcement actions for the breach of regulations relating to cookies.

Lack of information

On 7 December 2020, the CNIL fined Amazon and Google for placing advertising cookies on users' devices without providing adequate information as required by Article 82 of the French Data Protection Act. In relation to Amazon, the CNIL found that the cookie banner on the French website (*www.amazon.fr*) did not clearly explain that cookies placed on users' computers were mainly used to display personalised advertisements. The CNIL also noted a lack of information for users who visited the French Amazon website after they had clicked on an advertisement published on another website. The same cookies were placed but no information was provided to the users. As regards Google, the CNIL found that the cookie banner on the French website (*www.google.fr*) did not provide users with any information regarding the cookies that had already been placed on their computers when arriving or landing on the website.

Lack of consent

The CNIL observed that when a user visited the French Amazon website, cookies were automatically placed on the user's device. Several of these cookies were used for advertising purposes. These cookies are non-essential and can be placed only after the user has given consent. The same rationale applied to the French Google website. In addition, when a Google user deactivated advertisement personalisation, one of the advertising cookies was still stored on their device.

Separately, the CNIL's sanctions committee imposed a financial penalty against the French retailer Carrefour France and Carrefour Banque for, among other breaches, lack of consent, because when a user connected to the www.carrefour.fr or www.carrefour-banque.fr websites, several cookies were automatically placed on their terminal, before the user took any action. Considering that some of these cookies were used for advertising purposes, consent should have been sought before storing the cookies on the device.

advertising. With that in mind, the CNIL has recently reiterated in its 2021 enforcement priorities that it is actively focusing on cookie enforcement (*www.cnil.fr/fr/cybersecurite-donnees-de-sante-cookies-les-thematiques-prioritaires-de-controle-en-2021*). The CNIL reiterated its position in a set of frequently asked questions issued on 18 March 2021, in which the CNIL also confirmed that cookie audits will begin in April 2021 (*https://cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs*).

The CNIL has taken various enforcement actions targeting the use of cookies, including in late 2020 when it issued several high-profile fines for cookie non-compliance (*see box "CNIL cookie enforcement actions"*). The CNIL's enforcement actions consider three main criteria:

- The scope of the alleged breach; for example, the use of cookies, the user's information and consent.
- The scale of the impact; for example, the reach of the websites and the large-scale impact on French users.
- The financial benefits of the alleged breach; for example, when the company derives profits as a result of the alleged breach.

Court rulings on cookies

In conjunction with applicable law, regulatory guidance and enforcement action by DPAs, attention must also be paid to decisions of national courts and the European Court of Justice (ECJ), which continue to shape the law regulating cookies. A key decision in this regard is *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucher verbände - Verbraucherzentrale Bundesver band eV*, where the ECJ confirmed that consent obtained through pre-ticked cookies consent boxes is not valid consent under the GDPR (*C-673/17; www.practicallaw.com/w-022-5053*).

For the purposes of the GDPR, only active behaviour with a view to giving consent will suffice. In *Planet49*, the ECJ also clarified that users must be informed about the duration for which a cookie will be stored on their device and which third parties may have access to those cookies. These requirements go to one of the GDPR's core principles: that an individual must be able to determine at the outset the consequences of giving their consent.

It is also vital that organisations consider class action-style litigation claims in tandem with the increased appetite of DPAs to issue further cookie-related enforcement actions (*see box "Data class actions and cookies"*). This two-pronged risk defines the context in which organisations should approach their cookies compliance.

Data class actions and cookies

Organisations should be aware of another upcoming threat: data-led class action law suits (*see feature article "Data class actions: the outlook after Morrison", www.practicallaw.com/w-026-2617*). The possibility of class action style claims arising out of violations of the EU General Data Protection Regulation (*2016/679/EU*) (GDPR) has been a hot topic for some time and given the widespread use of cookies, cookies-related violations present a growth area for litigants. This is evident in recent parallel suits brought against software companies Oracle and Salesforce in the Netherlands, as a class action, and in the UK, as a representative action.

The technology giants have been accused of breaching the GDPR through their use of cookies to offer real-time bidding of advertising space to advertisers. The claimants assert that dynamic advertisement pricing services, by their very nature, fall short of the requirement of informed consent. With the outcome of the Dutch proceedings a long way off and the UK proceedings on pause until the Supreme Court's decision in the appeal of *Lloyd v Google LLC* later in 2021, it may take some time before the scope of class action style claims for cookies-related violations is gauged (*[2019] EWCA Civ 1599; see News brief "Data protection claims: a green light for representative actions", www.practicallaw.com/w-022-5323*).

GDPR ENFORCEMENT MECHANISM

The enforcement mechanism under the GDPR aims to be both practical and collaborative, prioritising the voice of one lead DPA while ensuring that each affected DPA has a means to contribute to the interpretation and enforcement of the GDPR.

The one-stop shop

Member states have their own data protection laws and regulations, and each member state has its own DPA. Businesses with operations in multiple EU countries are subject to the national laws and regulations of each member state. However, the reality is that dealing with each DPA in the country in which a business may have operations is burdensome and impractical.

The "one-stop shop" principle, set out in Article 56 of the GDPR, aims to address this problem and the realities of cross-border business by placing responsibility for enforcement action arising out of activities of the business across the EU, whether as controller or processor, with the DPA in the country of the business's main establishment. The term "main establishment" typically denotes an organisation's central administration, meaning that the DPA in that jurisdiction will serve as the lead DPA for any interaction with other DPAs, the European Data Protection Board (EDPB), which is the body responsible for advising the European Commission on data protection issues and issuing binding guidelines on the interpretation of the GDPR, and affected individuals. This lead DPA is entrusted with primary responsibility for regulatory oversight and enforcement action.

Consistency and co-operation

The one-stop shop principle and the lead DPA are supported by the following provisions of the GDPR:

- Article 60 on co-operation between DPAs (Article 60).
- Article 61 in relation to mutual assistance between DPAs (Article 61).
- Article 62 on joint operations between and among DPAs (Article 62).

For example, the lead DPA may request assistance from any concerned DPAs under Article 61, and DPAs in member states where a significant number of data subjects are likely to be affected have a right to participate in joint investigations and enforcement

Twitter Ireland and the EDPB

In January 2019, Twitter Ireland disclosed to the Irish regulatory authority, the Data Protection Commission (DPC), a bug that resulted in the private tweets of 88,726 users based in the EU and EEA being accessible to the wider public, without users' knowledge, between 5 September 2017 and 11 January 2019. It also disclosed that the bug was traceable to a code change made on 4 November 2014, but that no breach had been detected before 5 September 2017.

GDPR breach

Under Article 33 of the EU General Data Protection Regulation (*2016/679/EU*) (GDPR) (Article 33), a data controller is required to notify the relevant supervisory authority not later than 72 hours after becoming aware of a personal data breach likely to result in a risk to the rights and freedoms of affected data subjects. The DPC decided that, having failed to notify the DPC within 72 hours, Twitter was in breach of Article 33.

DPC investigation

As Twitter Ireland's lead data protection authority (DPA), the DPC reached a preliminary draft decision with respect to the breach in May 2020. Under Article 60(4) of the GDPR, the data protection authorities in eight EU member states (Austria, Denmark, France, Germany, Hungary, Italy, the Netherlands and Spain) raised objections to the decision. The objections concerned:

- The competence of the DPC as lead DPA.
- The qualification of the roles of Twitter Ireland and Twitter, Inc, as processor and controller respectively.
- The infringements of the GDPR identified.
- The existence of possible additional, or alternative, infringements of the GDPR.
- The lack of a reprimand.
- The calculation of the proposed fine.

The DPC replied to the objections in July 2020. The DPC reasoned that only the objections raised in relation to the calculation of the fine met the threshold put forward by Article 4(24) of the GDPR in so far as they related to the compliance with the GDPR of the envisaged action in relation to the controller or processor, and also set out the risks posed as regards the fundamental rights and freedoms of data subjects. Nonetheless, the DPC maintained that the level of fine was appropriate. As the DPC considered all other objections fell below the threshold of being relevant and reasoned, it refused to follow any of the objections raised by the eight DPAs.

In response, seven DPAs maintained their objections in full or partially. Consequently, in August 2020, the matter was referred to the European Data Protection Board (EDPB) under Article 65 of the GDPR (Article 65).

EDPB decision

In November 2020, in its first exercise under Article 65, the EDPB issued its binding decision on the dispute. The EDPB rejected the majority of the objections made against the DPC's decision. It agreed with the DPC's determination of the relationship between Twitter Inc and Twitter Ireland as a controller-processor relationship and that no additional articles of the GDPR had been breached. These objections were either unsubstantiated on available factual elements or failed to meet the threshold of being relevant and reasoned. In particular, the objectors failed to demonstrate how the decision of the lead DPA would pose significant risks for the rights and freedoms of data subjects or the free flow of data, or both.

However, the EDPB did accept the objections of the Austrian, German and Italian DPAs that the DPC's original proposed fine range of €135,000 to €275,000 did not meet the requirements of being effective, dissuasive and proportionate with respect to the infringing acts. While the EDPB agreed with the DPC that the character of the breach was negligent and not intentional, and that there were no systemic issues at Twitter, it agreed that the DPC had not given adequate weight to the fact that the affected data subjects had deliberately chosen to make their Tweets private and that, for a company such as Twitter for which the processing of personal data is at the core of its business, adequate procedures for documenting personal data breaches should have been implemented.

Further, the EDPB noted that a dissuasive penalty is one that has a genuine deterrent effect, citing the opinion of Advocate General Geelhoed in *Commission v France,* which stated that "effective" should mean that there is a high risk that non-compliance will be detected and sanctions would be imposed that would remove any benefit of the non-compliance, so that non-compliance is rendered economically unattractive (*C-304/02*).

The EDPB found that the DPC's proposed fine of €135,000 to €275,000 was not sufficiently effective, as the DPC did not sufficiently substantiate how the fine addressed the requirements that it be dissuasive and proportionate. It noted that the cap for the fine of 2% of Twitter Inc's global annual turnover meant that the maximum amount of the fine was $60 million, and that there was no clear motivation for the DPC's choice of the proposed fine of between €135,000 and €275,000 only, as the DPC did not explain the particular considerations that led to its decision.

The EDPB therefore concluded that the fine did not meet its purpose of being an appropriate corrective measure and remitted the decision to the DPC for it to decide on a fine that would meet the Article 83(1) of the GDPR requirements of being effective, dissuasive and proportionate.

DPC revised fine

The DPC, having regard to the EDPB's concerns, maintained that the infringements of the GDPR could be deemed moderately serious, as they pertained only to a failure to notify the breach on time, and adequately document the breach, in the final decision it issued on 9 December 2020. It decided to pay "particular regard to the nature, gravity and duration of the infringements concerned, taking account of the nature, scope and purpose of the processing and the number of data subjects affected". The DPC settled on an administrative fine of €450,000, stating that the amount would be effective, proportionate and dissuasive, taking into account all of the circumstances of the case.

measures under Article 62. In the event that the eventual decision of the lead DPA is objected to by DPAs other than the lead DPA, those DPAs can intervene through recourse to the consistency and co-operation mechanism.

The co-operation mechanism operates under Article 60(4), which provides that where an infringement of the GDPR affects data subjects in multiple jurisdictions, supervisory authorities in those jurisdictions are entitled to make a relevant and reasoned objection to the draft decision of a lead DPA.

The consistency mechanism states that DPAs may refer issues that implicate multiple member states to the EDPB (*Article 63, GDPR*) (Article 63). Under Article 64 of the GDPR, the EDPB must issue an opinion should a DPA wish to undertake certain actions. To resolve any disputes, including as to which DPA is the lead DPA, the resolution process under Article 65 of the GDPR (Article 65) is engaged, under which the EDPB is required to issue a decision on the matter for consistency.

To date, the dispute resolution process of the GDPR has been engaged just once: following a January 2019 data security incident involving the social networking platform, Twitter (*see box "Twitter Ireland and the EDPB"*).

Tensions ahead?

The first exercise of the Article 65 dispute resolution mechanism in the Twitter Ireland case offers an important insight into GDPR enforcement and the divergent outlook of DPAs concerning breaches of the GDPR.

The response of member state DPAs to the Irish Data Protection Commission (DPC), such as the German DPA's recommendation of a fine between €7.3 million and €22 million, demonstrates EU DPAs' appetite to see meaningful enforcement for breaches of the GDPR. Their objections send a clear message that, in the view of other DPAs, fines should have a genuine deterrent effect that is directly sensitive to the financial means of the infringing organisation.

The Twitter Ireland dispute also provides an insight into the approach of the DPC, which plays a central role in the GDPR enforcement of the most high-profile organisations as a consequence of Ireland being the place of European domicile for some of the world's biggest technology companies, including Google and Facebook.

Global revenue for Google and Facebook in 2019 was approximately $160 billion and $70 billion respectively, meaning that a 2% fine translates into figures ranging from $1.4 billion to $3.2 billion. The immediate response to the DPC's eventual, revised fine of €450,000 questioned whether it would, in practice, discourage other companies, in particular Big Tech companies from committing the same types of infringing acts.

The EDPB's decision in Twitter Ireland also revealed its difficult balancing act. On the one hand, some authorities, like the German DPA, consider that only a fine that is so high it would render the illegal data processing unprofitable would act as a genuine deterrent. On the other hand, it is clear that some authorities, like the DPC, have reasons to be more accommodating. The EDPB took these competing positions into account in agreeing with certain of the objections raised and disagreeing with the DPC on multiple aspects of its decision.

However, on the sensitive issue of the appropriate amount for the fine, the EDPB decided to remit the case back to the DPC for final determination, allowing the DPC to be the final arbiter. The DPC duly increased its initial proposed fine, indicating that it had taken the EDPB's decision into account and that the increased fine was around a 67% increase on the upper level of the range previously proposed.

As the first fine levied against Big Tech by the DPC, it is too early to draw conclusions on what this administrative fine may say about the DPC's future approach to enforcement. It is clear that various DPAs will continue to try to object to any perceived soft touch approach to enforcement. However, whether the EDPB will adopt similarly tactful decisions remains to be seen.

Article 65 provides that the EDPB's binding decision "shall concern all the matters which are the subject of the relevant and reasoned objection", which must include the appropriate range for a fine, should it be a matter subject to objection. That the EDPB chose to permit the DPC to make its own adjustment to the final administrative fine may be an indication of the EDPB's unwillingness to determine a matter as sensitive as the precise gravity of the infringement. Indeed, the EDPB tucked away in a footnote a reference to *Marine Harvest ASA v Commission*, one of many cases where the EU courts have indicated that the gravity of an infringement must be assessed in the light of numerous factors, such as the circumstances of the case, its context and the dissuasive effect of fines, although no binding or exhaustive list of the criteria to be applied has been drawn up (*T-704/14; www.practicallaw.com/w-011-7138*).

There is no doubt that further disputes will be raised under the co-operation and consistency mechanism. If DPAs are permitted to continue to impose fines that are perceived to be lenient, this may lead to a perception that the one-stop shop principle establishes jurisdictional "safe havens" in which organisations may benefit from a less exacting application of the GDPR by the relevant DPA, without effective intervention from the EDPB. This type of forum shopping could undermine the one-stop shop principle and the enforcement of the GDPR, evolving into a new factor for companies to consider when deciding on their European headquarters: whether a jurisdiction is considered to be a regulatory haven.

The result may be that tension between DPAs will increase rather than reduce through the co-operation and consistency mechanism, with the recent war of words between Ulrich Kelber, Germany's Federal Commissioner for Data Protection, and Helen Dixon, the Data Protection Commissioner for Ireland, exemplifying the likely direction of travel. In response to the Irish Commissioner's contentions that certain DPAs failed to understand key concepts with respect to the one-stop shop mechanism, the German Commissioner responded that the Irish Commissioner's "one-sided" views left the Irish DPA isolated from other EU DPAs and drew attention to the backlog of cases before the Irish DPA.

Far from facilitating co-operation, it seems that the one-stop shop mechanism is fast becoming a source of tension that will dominate discourse around the enforcement of the GDPR in the years to come.

INCREASED ENFORCEMENT EFFORTS

It is clear that DPAs are gearing up for increased activity in 2021, particularly in view of the ruling of the ECJ in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, known as *Schrems II*, in relation to which the fallout still remains unclear (*C-311/18; see News brief "Schrems II and data transfers: cast adrift*

in a sea of uncertainty", www.practicallaw.com/w-027-1214). In *Schrems II*, the ECJ ruled on two key data transfer mechanisms, invalidating the EU-US privacy shield for data transfers to the US and imposing enhanced due diligence on parties using the EU standard contractual clauses (SCCs).

Under *Schrems II*, where this type of enhanced due diligence determines, on a case-by-case basis, that the laws of the data importer's country do not provide essentially equivalent protection of personal data to that guaranteed under EU law, supplementary measures must be implemented. If the imposition of supplementary measures would still not provide essentially equivalent protection with respect to the data importer's country, the data transfer must be suspended. The EDPB has since provided guidance on assessing the laws of third countries and the form that supplementary measures may take, but market practice has yet to emerge (*https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf; https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf*). This grey area leaves ample room for enforcement action.

Irish DPC

In this respect, the DPC is naturally positioned as one of the most influential DPAs in the EU. As discussed above, numerous Big Tech companies have set up their European headquarters in Ireland. Activity for the DPC is consequently high: in its 2020 annual report (2020 report), the DPC revealed that it had handled a total of 10,151 cases and 6,673 data security breach notifications in the past year (*www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2020-annual-report*). The most frequent cases were queries and complaints, including access and deletion requests and concerns about direct marketing. The 2020 report also noted a number of inquiries with cross-border implications, including the Twitter case, Ryanair and Groupon (*see "GDPR enforcement mechanism" above*).

However, the DPC's enforcement priorities were more opaque, with the 2020 report stating in broad terms that, while after-the-event enforcement by the DPC will always play a central role in the discharge of its regulatory functions, the DPC is also mindful of the importance of encouraging compliance at source. The DPC also noted in passing that enforcement efforts would continue, with cookies being a key focus of its activities in 2021. This was reflected in a speech by the Irish Data Protection Commissioner, Helen Dixon, at a conference in late 2020, in which she was hesitant to list the DPC's enforcement priorities as enforcement is often more reactive than proactive.

In the 2020 report, the DPC noted the number of ongoing investigations into multinational technology companies based in Dublin that are due to be finalised in 2021. The issues being examined in the investigations are diverse. However, a number of investigations are focused on ensuring that companies have discharged their GDPR obligations by processing personal data only where they have a lawful basis to do so and by providing adequate prior information in their privacy notices in light of the GDPR transparency principle.

To help manage the caseload and bring in additional members of staff, and to implement IT infrastructure, the DPC reported a budget of almost €17 million for 2020, an increase of €1.6 million on its 2019 budget.

French CNIL

On the continent, the CNIL's budget and headcount has also recently increased. The budget of the CNIL increased by 8% from 2019 to 2020, reaching more than €20 million. By way of comparison, the CNIL's budget remained flat from 2015 to 2019. In addition, the French Budget Act for 2019 approved the creation of 15 new full-time positions at the CNIL to take on an increased workload due to the GDPR. Accordingly, the CNIL headcount increased by 12.5% from 2018 to 2020. By way of comparison, only two new positions were created between 2016 and 2018.

Beyond cookie enforcement, on 2 March 2021, the CNIL announced that it will actively focus its control activities on two areas in 2021: website cyber security and the security of health data.

Regarding health data security, on 12 March 2021, the Conseil d'Etat, France's highest administrative court, held that personal data used to book COVID-19 vaccinations through the Doctolib platform and hosted by Amazon Web Services Luxembourg, were sufficiently protected under the GDPR because the hosted data did not include medical data and because sufficient safeguards, both legal and technical, were put in place in case of a request from US authorities.

With respect to cyber security, the CNIL's objective is to verify the security level of French websites that generate the highest volume of traffic, with a focus on data collection forms, the https protocol and compliance with the CNIL's recommendation on passwords. The CNIL also announced that it will question organisations on their strategies against cyber attacks, such as ransomware. With respect to health data security, the CNIL announced that it will pursue the audits that were launched in 2020 in light of the increasing digitisation of the health sector, such as access management to electronic patient files, platforms to book medical appointments and personal data breaches in care facilities.

UK ICO

Although no longer an EU member state, the UK's DPA, the ICO, will remain the DPA for any international organisations with a UK presence. The ICO notes that there has been an increase in incidents and continues to actively enforce the UK GDPR. In its statistics for 1 July 2020 to 31 October 2020, the ICO received 2,594 notifications of data breaches (*https://ico.org.uk/action-weve-taken/data-security-incident-trends/*). The most common breach was phishing, and the most common cause of the breach was misdirected email.

In view of the ICO's willingness to fine British Airways and Marriott Hotels, there will certainly be increased action in future. It should be noted, however, that the UK Information Commissioner, Elizabeth Denham, is stepping down at the end of her term in October 2021. With the ICO's strategic plan, technology strategy, and international strategy all coming to an end in 2021, the new Commissioner may yet steer the ICO towards new horizons.

A CHANGED LANDSCAPE

When the GDPR came into force, it was understood that a seismic shift in the EU's data protection landscape would follow. In light of the trends in the enforcement of the GDPR, it must be said that this has come to pass. As is evident from both the efforts being directed towards cookies enforcement and the evidence that DPAs in certain member states intend to continue to be proactive in their

Related information

This article is at practicallaw.com/w-030-5470

Other links from uk.practicallaw.com/

Topics

Compliance: data protection	topic/1-616-6178
Cookies	topic/5-616-6218
Data protection: general	topic/1-616-6550
Data protection offences	topic/1-607-9647
Data sharing	topic/2-616-6187
Direct marketing: data protection	topic/9-616-6179
GDPR and data protection reform	topic/7-616-6199
Information technology	topic/5-103-2074
Sanctions and remedies: data protection	topic/0-616-6193
Technology: data protection	topic/8-616-6207

Practice notes

Cookies: UK issues and the impact of GDPR and DPA 2018	w-016-7485
Data security under the UK GDPR and DPA 2018	w-013-5138
Data subject rights (UK)	w-024-3178
Demonstrating compliance with the GDPR	w-005-2644
Ensuring data protection compliance	w-012-9916
Overview of data sharing arrangements (GDPR and DPA 2018) (UK)	w-018-8492
Overview of GDPR: UK perspective	w-013-3757
Overview of EU General Data Protection Regulation	w-007-9580
UK GDPR and DPA 2018: enforcement, sanctions and remedies (UK)	w-005-2487

Previous articles

Data protection officers: a many-faceted role (2021)	w-029-4571
Data class actions: the outlook after Morrison (2020)	w-026-2617
Data protection: privacy by (re)design (2019)	w-018-6087
E-Privacy Regulation: developing slowly (2019)	w-020-8272
GDPR one year on: taking stock (2019)	w-020-0982
General Data Protection Regulation: a game-changer (2016)	2-632-5285
Compliance for UK cookies: the deadline approaches (2012)	3-518-9542

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

enforcement efforts, there is a clear desire to see meaningful, effective enforcement of the GDPR in the EU and the UK.

This has been paired with a more prophylactic approach to GDPR violations, with DPAs and the EDPB taking on a far more vocal role since the GDPR came into force. This is reflected in the broad range of guidance, FAQs, opinions and statements that DPAs and the EDPB release, with the explicit intention of helping organisations to avoid violations of the GDPR and to stay on track with their GDPR compliance journey.

Naturally, as the prominence of DPAs has grown, so too have competing views on how the GDPR should be implemented and enforced. This tension between DPAs looks certain to shape the future enforcement of the GDPR. Further, the post-Brexit potential for divergence between the DPAs and the ICO will be relevant to companies with cross-border processing activities across the EEA and the UK, which may find that they are subject to dual enforcement action under the EU GDPR and the UK GDPR, respectively. The ICO is no longer part of the EU GDPR's consistency and co-operation mechanism and is, in essence, free to enforce the UK GDPR as it deems appropriate. Therefore, breaches of the EU GDPR and the UK GDPR that relate to inter-EEA-UK processing activities risk the possibility of "double jeopardy".

That said, the ICO's draft guidance on regulatory action published in October 2020 states that it will ensure that any administrative penalties issued will be proportionate (*https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf*). In addition, even in the absence of an official framework, there are incentives for co-operation between the ICO and the EU DPAs. The EU-UK trade and co-operation agreement between the UK and the EU keeps the door open for a deepening of the relationship, requiring collaboration through dialogue, the exchange of expertise and co-operation on enforcement (*see Briefing "UK data protection and the EU-UK trade agreement: where does the UK go from here?", www.practicallaw.com/w-029-3484*). Although this does not rule out the possibility of parallel enforcement action, it should bring some comfort to organisations that conduct cross-border processing activities in the EEA and the UK. The real test will come when the theory is put into practice.

The trends identified should give organisations plenty of food for thought when assessing their current and future compliance with the GDPR. With the threat of data protection based class action-style proceedings on the horizon, there has never been a more important time to ensure that their data protection and cyber security affairs are in order.

Bruce Macaulay is a partner, Eve-Christie Vermynck is counsel, Oscar Tang and Daniel Millard are associates, and Angus Goalen is a trainee solicitor, at Skadden, Arps, Slate, Meagher & Flom (UK) LLP. Aymeric Boëlle is an associate at Skadden, Arps, Slate, Meagher & Flom LLP in Paris, France.