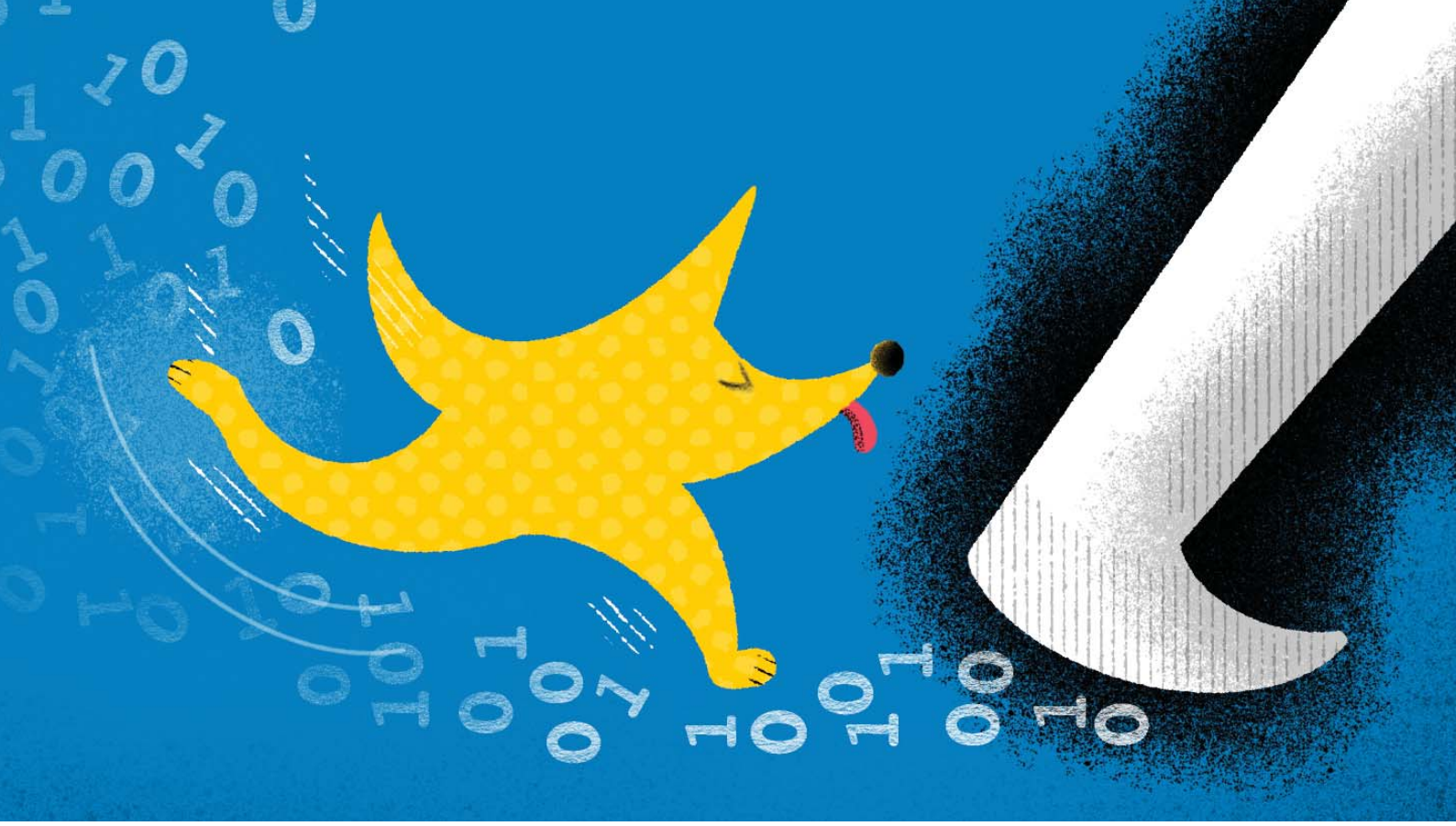

GDPR ONE YEAR ON
TAKING STOCK

Kate Brimsted and Tom Evans of Bryan Cave Leighton Paisner LLP look back on the 12 months since the General Data Protection Regulation (*679/2016/EU*) came into force and the key lessons learned so far.

Who could have imagined that a data protection-related acronym would become a household word? In the peak month of May 2018, "GDPR" was searched more often on Google than either Beyoncé or Kim Kardashian according to a European Commission (the Commission) publication (*https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf*). Added to this, for much of 2018, data protection was hitting the business news headlines on a weekly, if not daily, basis.

To a certain extent, that has not changed in 2019. The continual increase in identity theft makes this a more recognisable phenomenon and means that data breaches are routinely covered by the press. The extent of government and state surveillance of citizens was laid bare by Edward Snowden's whistleblowing revelations in 2013. Now the conversation has moved to the private sector, parts of which have embraced profiling and artificial intelligence (AI) for commercial advantage, so much so that the term "surveillance capitalism" has been coined, which continues to create waves and fuel an evolving public debate around privacy.

Now that we have reached the first anniversary of the General Data Protection Regulation (*679/2016/EU*) (GDPR) coming into effect, this is an appropriate point to take stock and reflect on the experiences following the EU's biggest shake up of data protection regulation to date. This article looks at what has changed, what has not and some of the more surprising outcomes.

STATUS QUO AND ENFORCEMENT

Without wishing to be cynical, it was the setting of maximum fines at the higher of 4% of annual global turnover or €20 million which signalled the seriousness with which EU lawmakers viewed data protection rights (*see feature article "General Data Protection Regulation: a game-changer", www.practicallaw.com/2-632-5285*). That alone probably did more than anything else to focus corporate and public sector attention on GDPR compliance.

In principle, every organisation within scope of the GDPR was required to be compliant from 25 May 2018. In practice, the far-reaching requirements imposed by the GDPR and the challenges of implementing it into operations, including situations where the practical requirements were uncertain, meant that many organisations considered that they had not completed their GDPR preparations by that date. Indeed, many are still working through them, with contractual negotiations with vendors having a very long "tail" (*see "Contractual and transactional trends" below*).

Incomplete reforms

The updating of the EU's digital laws as part of the digital single market initiative is only partially completed, and delays to e-privacy reforms have led to an unexpectedly uncertain regulatory environment which has thrown up challenges and opportunities that were not foreseen when the package was agreed (*see News brief "A digital single market: the European Commission unveils its strategy", www.practicallaw.com/7-614-4193*). The long-overdue E-Privacy Regulation, which will replace the E-Privacy Directive (*2002/58/EC*) and which was intended to come into force simultaneously with the GDPR, is still in draft and working its way through the EU's legislative process.

The draft has been the subject of heavy lobbying since its original proposal in January 2017. Jan Phillipp Albrecht, the German MEP who helped to steer the passage of the GDPR, has described the lobbying as unprecedented, and said that the tone adopted by lobbyists has been "radical" and "over-exaggerated". Despite both the European Data Protection Board (EDPB) and the Commission leading calls in May 2018 for the updated legislation to be adopted swiftly, there remains little clarity over when this will happen.

The EDPB released a statement on 12 March 2019 calling on the EU legislators to intensify their efforts towards adopting the E-Privacy Regulation and urging the EU member states to "proceed to the finalisation of their negotiating position without further delay". At the time of writing, the Brexit process is continuing, which can also be expected to consume the attention of the member states, not to mention the negotiations over post-Brexit trade. The EU parliamentary elections in May 2019 also inevitably divert attention away from this matter.

The unsettled e-privacy environment has had a disproportionate impact on the patterns of enforcement and regulatory investigations by the supervisory authorities, which are still required to enforce the law and have received a number of high-profile complaints from consumer rights groups and privacy campaigners. Indeed, the four complaints regarding online profiling submitted by NOYB (a non-profit, digital rights organisation established by Max Schrems), simultaneously to supervisory authorities in Austria, Belgium, France and Germany on 25 May 2018 set the tone for the prominent focus by campaigners and regulators alike in this field. A number of other similarly high-profile, pan-European complaints have followed.

For their part, governments in the UK and Ireland have appeared willing to provide the resources necessary to police the new regulatory framework (*see box "Increased resources"*).

Fines under previous regime

With supervisory authorities raising headcounts and maximum fine levels increasing, one might have expected to see a number of high-profile enforcement actions to be taken within the first year of the GDPR coming into force. The reality has been less dramatic. However, there has been a high volume of self-reports as a result of the compulsory breach notification requirement across all sectors since 25 May 2018. In addition, high-profile representative complaints against global social media companies and data brokers have been made to supervisory authorities in multiple jurisdictions (*see "Incomplete reforms" above*). However, the underlying situations tend to be complex, even where it is apparent that a breach has occurred and it is expected to take considerable time and resources to carry out regulatory triage in relation to the breadth and depth of matters raised with the supervisory authorities. At this point, it is inevitable that events have already occurred that will lead to substantial GDPR fines, even if they are not necessarily yet in the public domain.

In the 12 months since the GDPR's introduction, the vast majority of data-related enforcement actions taken by the Information Commissioner's Office (ICO) have concerned the now-repealed Data Protection Act 1998 (DPA 1998) and the Privacy and Electronic Communications Regulations 2003 (*SI 2003/2426*) (2003 Regulations). The ICO has yet to issue a monetary penalty notice for a breach of the GDPR. However, even though a number of data breaches have hit the headlines in the last year, thorough investigations take time to conduct. It is too early to judge at this stage how the ICO and other regulators will wield their powers when the results of these investigations emerge at the end of the waterfall and, in particular, how high the fines may be.

A recent enforcement action brought by the ICO against Grove Pension Solutions Limited (Grove) indicates that the regulator continues to take an uncompromising line where it considers that a serious infringement of the law has taken place. Grove had sent approximately two million emails to individuals without having obtained consent, but had taken advice from both a data protection consultancy and a lawyer. Although there are indications that the ICO took this advice into account as a mitigating factor, it fined Grove £40,000 for infringing the 2003 Regulations.

Related enforcement

The ICO has also been quick to exercise its powers in relation to the data protection fee which arises under the Data Protection Act 2018 (DPA 2018) and the Data Protection (Charges and Information) Regulations 2018 (*SI 2018/480*). In November 2018, the ICO began to issue notices of intent to fine organisations across a range of sectors including business services, construction, finance, health and childcare. These notices were issued for failing to pay registration fees following expiry of notifications under the DPA 1998. The ICO has suggested that more fines are soon to follow. In all, by the close of November 2018, the ICO had issued

Increased resources

In both Ireland and the UK, substantial funds have been made available to increase the headcount of the national supervisory authorities for data protection.

The budget for the Irish Data Protection Commission has reportedly gone up to €15.2 million, representing an increase of 800% since 2014. In the UK, the Information Commissioner's Office now has approximately 700 employees.

The Information Commissioner, Elizabeth Denham, has been very visible over the last year, with multiple appearances before parliamentary committees and inquiries, an increased media presence, the award of a CBE and appointment as chair of the International Conference of Data Protection and Privacy Commissioners.

Dutch data protection authority fines

On 12 March 2019, the Dutch data protection authority set out an indicative four-tiered structure for fines relating to breaches of the General Data Protection Regulation (*679/2016/EU*) (GDPR), based on the type and severity of the breach at issue:

Category	Fine	Offence
1	Up to €200,000	This band relates to simple GDPR violations such as a controller failing to publish the contact details of their data protection officer.
2	Between €120,000 and €500,000	This band applies to failures in fulfilling requirements applicable to processing activities, including failure to enter into data processing agreements with processors, or applying inadequate security measures to personal data.
3	Between €300,000 and €750,000	This band covers instances such as violating the GDPR's transparency requirements, failing to notify breaches and failing to co-operate with the Dutch authority. This penalty band is intended to tackle more serious wrong doing.
4	Between €450,000 and €1 million	The highest band relates to infractions such as unlawfully processing special category data and failing to comply with the Dutch authority's specific orders. Fines above the €1 million level can still be handed out where it is considered that the level of wrongdoing exceeds a category four sanction.

more than 900 notices of intent to fine, with more than 100 penalty notices being issued in this first round. The maximum sanction for failure to pay the fee is capped at £4,350, which is far below the level of fines possible under the GDPR.

Elsewhere in the EU, national supervisory authorities continue to develop guidance regarding when it is appropriate to take enforcement action (*see box "Dutch data protection authority fines"*). Guidance at a high level was also issued by the EDPB ahead of the GDPR (*https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237*).

Civil liability

Civil liability for data protection claims is not new in principle. The GDPR has, however, introduced the ability for not-for-profit bodies to bring representative actions on behalf of groups of individuals. While it remains too early to assess the implications of this, it appears inevitable that the patchwork of legal systems and approaches across the EU will continue to give rise to diverging results.

Recent cases before the English courts may provide an indication of the direction of travel for claims relating to data breaches. Arguably the most notable of these is *Wm Morrison Supermarkets Plc v Various Claimants,* in which the Court of Appeal found Morrisons vicariously liable for the actions of a rogue employee who had posted personal data relating to approximately 100,000 employees online (*[2018] EWCA Civ 2339; see News brief "Morrisons' liability for rogue employee: an apple of discord", www.practicallaw.com/w-017-7358*). There was little fault to be assigned to Morrisons in the circumstances, with the court noting that Morrisons had done as much as it reasonably could have to prevent the employee's actions and that the employee was motivated to cause reputational and financial damage to Morrisons.

Clearly, this case has implications for the doctrine of vicarious liability as a whole. In the specific context of data-related claims, however, the court noted that while many of the high-profile data breaches reported in the media might "lead to a large number of claims against the relevant company for potentially ruinous amounts", the solution to this was to obtain insurance. The court considered that the availability of insurance was a valid answer to the "Doomsday" or "Armageddon" arguments put forward on behalf of Morrisons.

It remains to be seen whether the judgment will lead to damages being awarded to the individuals affected by the breach, particularly since the Supreme Court recently granted permission to appeal. If upheld, the Court of Appeal's judgment would set a worrying precedent for employers and other companies facing a data breach, as well as having an impact on the insurance market, through increased demand for policies covering this type of risk.

DATA SUBJECT RIGHTS

Most organisations will have had experience dealing with data subject access requests (DSAR) made under the DPA 1998. These requests tend to be administratively burdensome, and remain the most common source of complaints received by the ICO, according to its most recent annual report. The strengthening of existing data subject rights and the introduction of new ones under the GDPR was inevitably going to prove a challenge and an increased burden for businesses, however, experience over the last year suggests that, while deletion requests are rising in frequency, DSARs remain the right exercised most frequently.

DSARs under DPA 1998

Data subjects have long had the right to access personal data processed about them by controllers in the UK. This right was established under the DPA 1998 and has been subject to judicial consideration in a number of cases before the English courts. The GDPR has not significantly amended the concept that lies behind the right, meaning that much of the old case law and guidance, such as the ICO's subject access code of practice published in 2017, remains applicable (*https://ico.org.uk/media/2259722/subject-access-code-of-practice.pdf*). This has been helpful for organisations that have found themselves on the receiving end of requests since the GDPR came into force.

The GDPR and the DPA 2018 do introduce important procedural changes, however, and these remain in need of clarification. At the time of writing, the ICO's code of practice has yet to be updated to reflect these changes, but a note has been added to the document to state that it will be updated soon. Once complete, this should help to manage any lingering uncertainties surrounding the application of subject access rights.

Key changes

Just like under the DPA 1998, individuals who submit a DSAR are entitled to receive confirmation as to whether their personal data is being processed by that controller, details of the processing and a copy of the personal data in the controller's possession. The GDPR has, however, bolstered these rights, namely through amending the procedural rules governing how DSARs are to be satisfied. The key changes include:

- No fee is payable for a DSAR unless the request is manifestly unfounded or excessive.
- Controllers have only one month to respond, with the possibility of extending a further two months in limited circumstances.
- A greater degree of information needs to be supplied, including in relation to retention periods and safeguards for transfers to non-EEA countries.
- DSARs no longer need to be made in writing.

The adjustment to the mandatory response time from 40 days to one month, with the possibility to extend this up to a further two months, continues to suffer from significant uncertainty as to the circumstances under which a controller is entitled to delay its response under Article 12(3) of the GDPR. This type of delay is allowed "where necessary, taking into account the complexity and the number of the requests". Guidance is awaited to help organisations establish when it is justified to delay responding to data subjects for up to three months.

Increase in requests

The abolition of the £10 fee for submitting a DSAR under the DPA 1998 was undoubtedly intended to remove a barrier that may have prevented, or at least deterred, individuals from validly exercising their rights in the past. Independent statistics on the number of DSARs being received are hard to come by, however, anecdotal evidence suggests that abolishing the fee has not made a great difference so far to the levels of DSARs received by organisations, which are primarily business-to-business requests. This may well be because those motivated to make a DSAR under the old regime would not have been put off by a relatively low fee.

While that may hold true for DSARs made by employees, for organisations with a significant consumer-facing operation and client base, the lack of a fee means the growth of protest or speculative DSARs is more likely. Based on the authors' experience and anecdotal evidence, higher levels of public awareness also appear to be fuelling an increase in requests for data deletion from individuals, that is, the right to be forgotten (*see News brief "Google decision: the right to be forgotten", www.practicallaw.com/3-568-9605*).

These deletion requests tend to be challenging to manage for many organisations, not least because individuals can have the firmly held misconception that the right is an absolute one. At the same time, an organisation needs to be fair and open in its response and when it explains the extent to which any deletion will, or will not, be taking place.

A further factor is the arrival on the scene of commercial third-party DSAR "aggregators" that are seeking to make DSARs easier to make for data subjects. These services offer a central point from which multiple DSARs can be sent on an automated basis on the individual's behalf to a number of large organisations. Should a response not be forthcoming, the next step would be to assist individuals to complain and possibly to demand compensation. This market can be expected to increase in size and, even apart from the growth in these third-party services, the first year of the GDPR has inevitably seen organisations having to put all their data-related policies and procedures to the operational test. This has been particularly visible in the area of data subject rights.

While remaining scarce, evidence showing whether the rights provided under the GDPR have led to more DSARs being made is beginning to emerge. Information provided by Nottinghamshire Police following a 2019 freedom of information (FOI) request shows that 2018 saw a significant increase of 23% in the number of valid DSARs being submitted (*www.nottinghamshire.pcc.police.uk/Document-Library/Public-Information/Meetings/Audit-and-Scrutiny-Panel/22nd-February-2019/Item-11-Force-Assurance-Report-on-Compliance-with-Freedom-of-Information-and-Data-Protection-Requests.pdf*). The increase in invalid DSARs submitted was substantially smaller, which is not surprising as the formal requirements for making these requests have also decreased.

Moreover, the evidence shows that as DSAR numbers jumped in 2018, the police force became more efficient in responding to DSARs within the statutory timeframe, despite that falling from 40 to 30 days. It is too early to tell whether this sample is representative of a wider trend, although the FOI response provides a positive outlook for how requests are being handled.

CONTRACTUAL AND TRANSACTIONAL TRENDS

Contractual provisions relating to data protection became a major area of focus for many organisations in the run up to 25 May 2018. Although the Data Protection Directive (*95/46/EC*) and the DPA 1998 had required a contract to be in place between a controller of personal data and any third party engaged as a processor, the GDPR's prescriptive list of obligations to include in these contracts threw the area into sharp focus. 12 months on, this appears to have had lasting implications.

Negotiations

The first implication is a simple one: data protection provisions are subject to heavier negotiation than ever before, and take on a more prominent role. Commonly, these negotiations centre around commercial issues, including liability caps, responsibility for determining security measures, and the extent of support that a processor will provide to a controller to assist it in meeting its obligations and who pays for this.

As the ICO notes in its guidance on contracts and liabilities between controllers and processors, the commercial aspects of the contract are a matter for the parties, so long as this complies with the GDPR (*https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/*).

While the dialogue has largely has shifted from GDPR-readiness to business as usual, market positions on these issues are still emerging, and so it remains common to see novel approaches taken.

Controller or processor

The second, and more fundamental, implication is that many organisations have revisited or reconsidered whether they act as either a controller or a processor. This is, again, not a new conundrum: companies and their advisers have long grappled with the distinction between the two roles. But the level of detail of the obligations that the GDPR requires to be imposed in contracts with processors has made it a distinction with more stark consequences, not least for the number of data processing agreements, commonly called DPAs, that are filling lawyers' inboxes. Over the years, both the Article 29 Working Party and the ICO have released guidance on the difference between the controller and the processor roles, however the distinction remains very fact-specific (*https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/*).

Where it is accepted that two parties both act as controllers, there are still contractual issues to consider. These are more nuanced, since the GDPR does not impose any specific provisions for contracts between independent controllers. In situations involving joint controllers, the GDPR requires an arrangement to be in place setting out the respective responsibilities of each party to comply with the legislation. The concept of joint controllership is imprecisely defined. It implies a close, mutually co-operative arrangement between two or more parties that may not accurately reflect the reality. There are also important legal reasons why multiple parties may seek to avoid creating a joint controller relationship, such as the possibility of incurring joint and several liability for breaches of the GDPR.

Where two parties each act as independent controllers, the ICO's pre-GDPR data sharing code of practice provides that it is good practice to have a data sharing agreement in place (*https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf*). Under section 121 of the DPA 2018, the ICO is required to issue a revised code on data sharing, however, the timing of its release is not currently known and it will be required to undergo consultation before it can be finalised. In addition to this good practice requirement, there may also be important commercial reasons why one controller would want to be aware of issues affecting the other, particularly in the new era of mandatory breach reporting.

DATA BREACHES

The introduction of mandatory data breach reporting requirements is a rare instance of EU data protection law playing catch-up with laws that are already in force in the US. The first victims of "breach fatigue" in the EU appear to have been the supervisory authorities, which found themselves deluged with notifications in the months following May 2018.

Reporting

In the UK, the ICO is understood to have received around 500 reports by telephone per week in the weeks after the GDPR came into force; this has since fallen to around 400 per month. Consistent with this, the Dutch data protection authority announced that it received over 20,000 reports in 2018. A number of high-profile data breaches have also made headlines following announcements made by those organisations to affected individuals, particularly consumers. According to information released by the Commission, between May 2018 and January 2019 41,502 breach reports were made to supervisory authorities across the EU, although some of these will include breach incidents which occurred before the GDPR came into force.

In contrast to US state-level data breach laws, where the trigger for notification tends to relate to the compromise of specific types of data such as social security numbers, the GDPR requires a personal data breach to be notified to supervisory authorities unless it is "unlikely to result in a risk to the rights and freedoms of natural persons". Affected individuals must also be notified if a personal data breach is likely to result in a "high risk" to their rights and freedoms.

These context-specific tests can be difficult to apply in the immediate aftermath of a

Related information

This article is at practicallaw.com/w-020-0982

Other links from uk.practicallaw.com/

Topics

Compliance: data protection	topic1-616-6178
Data protection: general	topic1-616-6550
Data security	topic8-616-6189
Data sharing	topic2-616-6187
Employee data, monitoring and privacy	topic5-200-0623
GDPR and data protection reform	topic7-616-6199

Practice notes

Data breach notification under the GDPR	w-013-5105
Data Processor Obligations under the GDPR	w-005-6153
Data Protection Act 2018: overview	w-014-5998
Data Subject Rights under the GDPR	w-006-7553
Data protection in corporate transactions (GDPR and DPA 2018) (UK)	w-014-9200
Overview of EU General Data Protection Regulation	w-007-9580

Previous articles

Data protection: privacy by (re)design (2019)	w-018-6087
Data protection in M&A: under lock and key (2018)	w-017-6243
Data use: protecting a critical resource (2018)	w-012-5424
General Data Protection Regulation: a game-changer (2016)	2-632-5285

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

breach being discovered, when it is often unclear whether, and to what extent, personal data have been compromised. The evidence suggests that in the year since the GDPR came into force, organisations have adopted a cautious approach, resulting in over-reporting to regulators.

Helpfully, this is an area in which supervisory authorities have been active in issuing guidance. In February 2018, the Article 29 Working Party (now replaced by the EDPB) issued its Guidelines on Personal Data Breach Notification under the GDPR (the guidelines) (*https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052*). In the UK, the ICO has published its own guidance on data breach notification, and has also provided a self-assessment tool online to allow organisations to assess whether a breach should be reported (*https://ico.org.uk/for-organisations/report-a-breach/*). Taken together, these resources provide a framework that allows organisations to assess the severity of any particular breach and then to infer from that whether reporting it to the regulator should be considered mandatory or not.

Record-keeping

As the dust settles on GDPR implementation, organisations face a challenge in ensuring that a degree of consistency exists between breaches that have been deemed reportable, and those that have not. For organisations with a mature privacy programme, records of processing may provide a useful starting point for the development of an objective breach appraisal methodology.

The EU Agency for Network and Information Security's (ENISA) recommendations for a methodology of the assessment of severity of personal data breaches sets out a framework for the holistic assessment and scoring of data breaches (*www.enisa.europa.eu/publications/dbn-severity*). Organisations that adopt a framework of this type may improve the consistency, and potentially the defensibility, of the reporting decisions that they take. Data breach drills are also effective in testing readiness for these incidents. It is important to remember that there is an internal record-keeping obligation in relation to breaches, whether they are reported to a supervisory authority or not.

Form of notification

Deciding whether to notify supervisory authorities and affected individuals is only half of the story. Once it has been determined that a notification should be made, it is important to consider the form that the notification will take, and the details that will be disclosed. In the UK, the ICO has made available a template breach notification form which can be populated and submitted, and will also accept notifications made by phone. Organisations using that latter route should keep in mind that what may start as a discussion about whether an incident should be reported may well morph into the actual report itself; discussions cannot be off-the-record once an organisation is named.

Whatever form a notification takes, organisations should be mindful of the fine line between disclosing information that is required by law, and voluntarily over-disclosing information that seems potentially relevant at the time, but which may not be helpful in the longer term. This is particularly true for listed companies and businesses in highly regulated industries, which may face dual reporting requirements; the ICO has memoranda of understanding in place with various regulators, and it is prudent to assume that anything disclosed to one regulator may find its way to others.

THE FUTURE

A year into implementation and considerable uncertainties remain over important aspects of the GDPR's interpretation, such as the jurisdictional reach and application of data subject rights. Important guidance continues to be released by the EDPB, some of which is capable of having a profound organisational impact at a point when organisations had hoped that the bulk of the effort had already been expended.

Add to this the uncertainties of Brexit, with the impact on data flows to the UK from the remainder of the EU and the future possible application of overlapping data protection regimes, not to mention the long-delayed E-Privacy Regulation, and it is clear that businesses will need to continue to be alert and invest in continuous compliance in this area.

Kate Brimsted is a partner, and Tom Evans is an associate, at Bryan Cave Leighton Paisner LLP.