2020 and Beyond: A New Decade of GDPR Enforcement

GDPR Masterclass
2020 and Beyond: A New Decade of GDPR Enforcement

As the new decade takes hold, we look at how the GDPR vastly reshaped data protection law for organisations throughout Europe and abroad towards the end of the 2010s, and how the data protection conversation may yet make the years ahead the new roaring 20s.

2019 in Focus: What did it mean for GDPR, and what’s ahead for 2020 – and beyond?

2019 quickly became the year of GDPR enforcement as many of the EU supervisory authorities began to properly deploy their new powers. In January, the CNIL (the French regulator) kicked off 2019 with a bang, having fined Google a record €50 million for failing to provide users with understandable and transparent information. In the summer, the UK Information Commissioner’s Office (“ICO”) announced two potential record breaking draft fines in July against British Airways and Marriott International, of £183 million and £99 million respectively, for security breaches.

The year concluded with the Austrian Data Protection Authority fining Austrian Post €18 million and the Berlin Commissioner for Data Protection and Freedom of Information fining a real estate company €14.5 million for various violations.

In Ireland, while the Data Protection Commission (“DPC”) has launched numerous statutory inquiries – roughly 60 as of January 2020 – it has yet to issue any fines. Approximately one third of these inquiries have been opened against large international tech companies anchored, i.e. with their main establishment under GDPR, in Ireland. However, given that inquiries are a necessary prerequisite before the DPC can issue fines under the Data Protection Act 2018 (“DPA”), the existence of such a large number demonstrates the high probability of fines being issued, in at least some cases, by the DPC once these inquiries conclude.

Equally, Commissioner Helen Dixon has made clear that the DPC plans to use the full range of her enforcement powers, rather than just imposing fines. This is unsurprising, given that fines can simply be paid and organisations then move on. On the other hand, prescriptive corrective measures from the DPC can direct organisations with respect to exactly what they can and cannot do with personal data. We also got a flavour for this in 2019 from the DPC’s investigation into the State’s Public Services Card Scheme, during which the DPC stipulated that the use of the card for various functions and by various state bodies must cease.

However, for the vast majority of organisations, 2019 will have seen less focus on dealing with DPC inquiries and potential fines, and much more focus on the day-to-day operation of GDPR compliance regimes. We take a look at some of these below.
Enforcement Trends:
From Private Actions to
Public Inquiries

There are different ways in which GDPR proceedings can arise in the EU. Broadly speaking, these can be divided into two types:

- Civil litigation, and;
- Regulatory enforcement.

One of the bigger trends of 2019 was an increase in private actions taken in Irish courts, and courts across Europe more generally, against organisations seeking compensation for alleged GDPR violations. While these actions have received much less publicity than the big, hot topic fines, they arguably have – and may continue to – present a greater risk for the vast majority of organisations than GDPR fines.

The option to bring civil litigation for damages in tort existed under the previous Irish data protection framework. However, the GDPR is designed to facilitate further civil litigation, which leads to some interesting points.

- First, it is worth noting that data subjects are entitled to sue before their home courts. This means that, in cross-border situations (e.g. an Irish financial services institution dealing with a German customer), an organisation may be sued outside of Ireland, notwithstanding the GDPR’s One-Stop-Shop principle.
- Second, the GDPR also allows NGOs to take representative actions on behalf of data subjects, which effectively comprise private enforcement actions.
- Third, damages are available for material and non-material damage. However, the precise nature of these terms is, as yet, unclear, and their interpretation needs to be considered by the Court of Justice of the European Union before any such clarity is agreed. So far, the damages awarded by courts across Europe have been nominal in many cases.

However, even nominal damages of a few hundred euro for a technical violation of the GDPR can rapidly lead to eye watering figures if such a technical violation could impact on all employees or customers of a business. These sorts of dispersed nominal damages have been a feature of US class actions for many years; however we may start seeing similar issues arising in Europe.

DPC enforcement has been the other big trend of 2019, and this is a space to monitor in 2020 and beyond. In practice, to date DPC enforcement can broadly be divided into two sorts of cases:

- Amicable Resolution ("AmRes") cases and;
- Statutory inquiries.

The AmRes cases comprise the vast majority of DPC enforcement actions, and arise where a data subject makes a complaint. Where the DPC considers that there is a reasonable likelihood of the parties to a complaint reaching an amicable resolution within a reasonable timeframe, it may take steps to arrange or facilitate the amicable resolution of a complaint. In practice, this may be facilitated at any stage of the complaint-handling process within the DPC, where the parties are willing to have the complaint handled in this way.

Statutory inquiries are a much more complex and involved procedure which essentially consist of two distinct processes – (1) the investigatory process, which is carried out by an investigator in the DPC, and (2) the decision-making process, carried out by a separate senior decision-maker in the DPC who has had no role in the investigatory process (usually the Commissioner).

In terms of fines potentially subsequent to these inquiries, the grounds for calculating these still remain unclear at this stage. The Irish approach will likely become clear by way of the DPC’s decisions and we expect Article 83 to provide key guidance to the DPC as it calculates fines. While we’ve seen some other European regulators publish guidelines on how they calculate (or will calculate) fines, so far, these guidelines are inconsistent.
So in summary, what’s on the DPC enforcement horizon for 2020?

So far, from what we’ve seen, the DPC’s style of enforcement under the GDPR has been somewhat similar to that seen before the GDPR came into force, particularly when it comes to evidence gathering. When conducting inquiries, the DPC’s preference throughout 2019 has been to write to companies asking them to voluntarily respond to certain questions to assist them with their investigations, while also seeking supporting documents. The DPC’s expectation of voluntary engagement will very likely continue, and it is likely that it will try not to have recourse to its mandatory enforcement tools like issuing information notices or appointing authorised officers to investigate complaints, unless the voluntary engagement process fails.

However, what is set to be interesting for 2020 is how the resource constraints at the DPC may lead to its use of some of the alternative and interesting tools available to it, such as (for example) the launching of joint investigations with other supervisory authorities into cross-border processing operations. Perhaps the DPC might also push more of the burden in its investigations on organisations by asking them to provide reports under Section 135 of the DPA, which enables the DPC to effectively outsource its work by requiring organisations to appoint independent reviewers to conduct an investigation and to prepare a report for the DPC. This process has real teeth, since it is a criminal offence not to cooperate with, or to try obstruct, the completion of such reports.

Security Breach Management

The management and notification of security breaches has been another hot topic over the past year, following a new set of mandatory breach notification rules introduced by the GDPR. In the first year of the GDPR alone (25 May 2018-25 May 2019), the DPC received 5,818 breach notifications, and it is likely that this strong trend will continue over the next year.

The definition of personal data breach is very broad; and so it is likely that the vast majority of organisations will have experienced a security breach of some sort, since an error as basic as sending an email to a wrong addressee is likely to be caught. Some lessons learned since the arrival of the GDPR on the breach management front have been:

• To prepare an incident response plan and, in some instances, simulate a breach to ensure effective operation and compliance with the GDPR in real life;
• To record every personal data breach and maintain a detailed breach register;
• To cure the vulnerability which caused the data compromise without delay;
• If acting as a data processor, to notify every security breach to the relevant controller without undue delay; and
• To notify the DPC of a breach without undue delay and, where feasible, not later than 72 hours after having become aware of the breach and to notify data subjects if it presents a high risk to individuals.

In practice, security breaches in a B2B context can give rise to significant liability concerns and issues concerning the relationships between the parties. In most cases, it is advisable that an organisation’s Data Processing Agreements (“DPAs”) take account of these potential liability issues.
Data Processing Agreements

One of the main practical consequences of the GDPR has been the increased requirements for data protection provisions in contracts. In practice, the need for DPAs has resulted in greater points for negotiation between parties, and some practical issues for day-to-day practices.

Over the past year, we have noticed a couple of trends when it comes to negotiating DPAs:

First, there is much more recognition from non-EU companies that "EU-style" DPAs have become a non-negotiable prerequisite of doing business with an EU company. In particular, US and Canadian companies have become very alert to these points and may have their own standard documents. Organisations should take care to ensure counterparties in other jurisdictions are similarly informed about the GDPR’s requirements before doing business.

Second, battle of the forms issues are starting to arise here. If both the supplier and the customer have their own template DPA, the question regarding whose paper/template DPA is to be used can often turn into a power play during negotiation stages on both sides. Organisations should be mindful of their objectives and whether these can still be achieved by agreeing that the other side’s template agreement can form the basis of a deal, provided that suitable amendments are made.

Third, it is important to remember that the GDPR’s rules on DPAs only apply where one side acts as a controller and the other side acts as a processor. While this is the default position in a service provider scenario, the classification of parties is something that needs to be specifically considered at the start of each transaction, and one needs to be mindful of deals where parties are acting more like partners – or joint controllers. In these cases, to comply with the GDPR template agreements need to be significantly amended to explain respective roles of parties – and the essence of those agreements must be made available to data subjects.

Data Exports

Important issues also arise where a European company (which is subject to the GDPR) proposes to transfer data outside the EEA. The GDPR permits the free flow of personal data within the EEA, while transfers of data outside the EEA are regulated. Brexit means that the UK will soon be outside the EEA so a significant piece of work for companies over the coming months will be needed to work out how to legitimise data transfers between the UK and Ireland after the expiry of the transition period.

Some non-EEA countries like Israel, Switzerland and New Zealand are white listed by European Commission adequacy decisions, so are treated as if they are part of the EEA when it comes to data exports. For non-EEA and non-white listed countries, there a few tools which most companies rely on including Binding Corporate Rules ("BCRs"), Standard Contractual Clauses ("SCCs") and the US Privacy Shield (for exports only to the US). Outside of these tools exports get much trickier since companies have to rely on narrow derogations found in Article 49 of the GDPR.

Based on a survey conducted by MHC, it appears that the most popular export mechanism in 2019 were SCCs – a data export mechanism which allows data to be transferred outside the EEA through certain contractual terms. BCRs are expensive and limited to intra-group transfers, while the Privacy Shield only applies to exports to certain participating US companies, and so a larger percentage of companies tend to rely on SCCs. However, the DPC has questioned the validity of SCCs and this case – the Schrems II case – is now before the CJEU with a decision due in 2020. This case largely focuses on US national security law, and whether data can validly be transferred to the US pursuant to SCCs given the obligations that US national security law imposes on certain companies.
Last month, Advocate General Henrik Saugmandsgaard issued a non-binding yet influential opinion on the validity of SCCs, suggesting that while, in his view, the SCCs framework generally provides a viable basis to export data from Europe, regard needs to be had as to whether, in certain cases, the data will be properly protected. In addition, while the Advocate General was firmly of the view that the court did not need to address Privacy Shield in the course of this case, he expressed serious doubts about the Privacy Shield’s validity.

For now, companies can continue to use SCCs, but there may be more bumps on the road. If the CJEU follows the AG’s Opinion, supervisory authorities, like the DPC, will still have the power to prohibit transfers to certain countries where it considers that data subjects’ rights are not fully protected after such exports.

Finally, if an organisation is using SCCs another practical point to bear in mind is that the European Commission is likely to issue new SCCs in 2020, given that the current SCCs are pre-GDPR and so need to be updated. Once the new documents are issued, organisations may need to update their old SCCs within a certain period of time.

Data Subject Rights

The GDPR gives data subjects a variety of rights regarding their personal data. These rights apply against data controllers and the GDPR prescribes how and when each right applies. These rights are contained Chapter III of the GDPR (Articles 12-23). Data subjects are provided with the rights such as the right of access, the right to be informed, the right to erasure, the right to object to processing of personal data, the right to rectification, the right of restriction of processing, the right to data portability, and rights in relation to automated decision making, including profiling.

Data subject rights must be responded to:

- “without undue delay”
- within one month of receiving the request at the latest with a possible two month extension if:
  - the request is complex; or
  - there are numerous requests.

The DPC’s 2018 annual report provided a breakdown of the types cross-border complaints received to the DPC through the One Stop Shop framework. The highest percentage of complaints received related to issues of consent (around 27%). This was followed by complaints concerning the right of erasure at 25%, and the right of access at around 18%.

The right to be forgotten

Since the adoption of the GDPR, we have seen a marked increase in the number of data subjects exercising the right to erasure under Article 17 of the GDPR, also known as the right ‘to be forgotten’ or the right to ‘deletion’.

It’s important to remember that the right to deletion is not an absolute right – it is a technical legal one, and only arises in certain cases.

When assessing a deletion request, a controller should consider a number of factors:

- First, has the right been triggered?
- Second, do any exemptions apply?
- Third, do we need to tell anyone about the request?
- Fourth, how do we operationalize this requirement?
Organisations must first assess if a valid erasure request has been made by a data subject. In other words does one of the pre-conditions to erasure apply? These are:

- Retention of the data is no longer necessary;
- Data subject withdraws their consent;
- Data subject objects to processing based on legitimate interests;
- The personal data has been unlawfully processed;
- Deletion is required to comply with a legal obligation; and
- The data was collected in relation to certain online services provided to a child.

The right to deletion must always be balanced against other fundamental rights and there may be circumstances under which an organisation could have grounds to refuse to grant an individual’s request to exercise their data protection rights. These exceptions include:

- Freedom of expression;
- Compliance with a legal obligation;
- Certain reasons of public interest (health, historical research etc…); and
- Establishment, exercise or defence of legal claims.

However, it is important to bear in mind that the controller must prove an exception applies.

In practice, in 2019 attempts have been made to use the right of deletion to remove lawful speech or commentary. These sorts of cases trigger the freedom of expression exception. Under the Irish DPA 2018, this exception is broader than the GDPR. Section 43 of the DPA 2018 makes clear that in the event of a conflict between the GDPR and the right to freedom of expression and information, the right to freedom of expression and information takes precedence. In some cases, companies are also relying on the “compliance with a legal obligation” exemption to decline certain deletion requests; e.g. where an attempt is made to delete sales records which need to be retained for compliance with tax law.

One area where we’ve seen companies run into difficulties is with the onward notification rules contained in Article 17(2) and 19. At a high level, these rules oblige data controllers who have shared a data subject’s personal data with third parties to tell those third parties about the deletion request, where possible. This is often overlooked in practice which can cause difficulties.

How best to operationalise deletion requests in 2020 and beyond?

Following the introduction of the GDPR, many organisations faced a spike in the volume of deletion requests they received. Effective management of deletion requests requires the putting in place of appropriate policies and procedures so as to enable companies to both determine how to respond to requests and, where required, to identify and delete the necessary personal data.

As Article 17 guarantees every data subject the right to “obtain the erasure of personal data concerning him or her without undue delay”, this means organisations must have workable erasure mechanisms in place. For example, a data controller planning to rely on consent should have a plan in place to cease processing upon a data subject’s withdrawal of consent.

If a valid erasure request is received and no exemption applies, then organisations will have to take steps to ensure erasure from systems. Those steps will depend on an organisation’s particular circumstances, its retention schedules, and the technical systems that are in place.

In all cases, when complying with erasure requests and communicating with the data subject(s), organisations should be clear with individuals as to what will happen to their data as a result of their request, including what will happen to data in backup systems.
What does the GDPR say here?

GDPR accountability obligations fall broadly into two buckets: the first being those that are clear to implement and clearly explained by the GDPR and supporting guidance. These “straightforward” accountability requirements include the maintenance of adequate records of processing activities. These records should outline:

- What categories of data subjects and personal data are being processed;
- The technical and organisational measures in place for the protection of the data,
- The name and contact details of the controller or processor where applicable;
- The purposes of the processing;
- The envisaged retention periods for the data; and
- A general description of the applicable security measures.

Organisations should check with their Data Protection Officer (“DPOs”), or whoever is otherwise responsible for data protection compliance, if this documentation is in place. If not, it should be prepared, both to comply with law and because the DPC will likely ask to see if they ever have cause to make inquiries.

In terms of other clear requirements, the GDPR imposes a specific obligation to conduct Data Protection Impact Assessments (“DPIAs”) before any high risk processing takes place.

Helpfully, plenty of guidance has been issued as to when DPIAs should be carried out, as well as how.

Similarly the GDPR requires that companies keep appropriate logs of any data security incidents that they may have suffered. So companies should properly document their assessment and response to a breach. In particular, if an organisation determines that a breach results in little or no risk to data subjects and decides not to notify the DPC, then this decision and its reasoning needs to be recorded since the DPC may ask for a copy of it at some stage.

Continued GDPR Compliance, 2020 and Beyond: Accountability and Governance Frameworks

Given that the GDPR has now been in effect for a while, organisations should be focusing on their compliance and ensuring that they have accountability documentation in place. Generally speaking, in the rush to get GDPR compliant in 2018, many organisations overlooked elements of the accountability principle. For instance, while some data protection impact assessments (“DPIAs”) were carried out in 2019, many companies are still figuring out how to implement DPIAs into their organisational framework. A trend for 2020 is undoubtedly going to be increasing compliance with the accountability provisions in the GDPR and this is going to be in part driven by regulatory expectations.
The second set of GDPR accountability requirements are vaguer, and so are trickier for organisations to implement. Article 5(2) of the GDPR lays down the principle that controllers must be able to demonstrate compliance with all the data protection principles in Article 5 (which are the core GDPR principles of purpose limitation, data minimisation, etc.). Article 24 requires controllers and processors to assess and to put in place measures to ensure and to be able to demonstrate compliance with the GDPR. Taken together, these provisions lead to an expectation, on the part of regulatory authorities that controllers put in place GDPR ‘compliance programs’.

A trend in 2019 has been uncertainty as to how organisations can best comply with these general accountability obligations. The takeaway here is that larger organisations are going to be expected to have a GDPR accountability and decision-making framework in place.

This might be best described as a governance structure which:

- starts at Board level and identifies what elements of decision-making that the controller is delegated and to whom;
- identifies the policies which these decision-makers have to follow;
- provides for oversight and reporting by these decision-makers. This includes oversight of all data processors that are engaged; and
- addresses how the DPO’s role interacts with those of the decision makers and the board.

The recording of important decisions concerning personal data processing will be an important aspect of these frameworks and the DPC frequently asks for evidence of these decisions when it investigates companies. For example, in the event that you decide not to follow the advice of your DPO, it is advisable that you should document your reasons for not doing so.

**Looking Ahead: The GDPR Horizon – 2020 and Beyond**

With all these key trends and takeaways in mind, organisations must continue to explore their position and continued responsibilities in terms of GDPR accountability and governance.

A good starting point is to assess, with those given responsibility for data protection issues within your organisation, whether a framework has been put in place to facilitate compliance with GDPR and DPC’s expectations. As above, these should be monitored and updated periodically as the privacy landscape looks set to continue to evolve over 2020.
About us
Our Privacy and Data Security Legal Team provides world-class expertise and strategic advice on all issues surrounding data protection law, privacy law and cyber-security compliance.

With a client base ranging from the world's best known data driven companies, to high potential start-ups and government institutions, we offer clients unparalleled global expertise coupled with detailed local knowledge.

Our expertise
• Data Protection
• Data breach incidents
• New technologies and Internet of Things
• Global Privacy Structure
• Investigations and Litigation
• Compliance and Accountability
• Law Reform

What others say about us
Our Privacy & Data Security Team
The team has “a lot of experience” and can “anticipate” issues.
Chambers & Partners, 2019

Our Privacy & Data Security Team
“The lawyers understand the issues and the pressures, are quite personable and are readily available at short notice.”
Chambers & Partners, 2019

Our Privacy & Data Security Team
The team has “incomparable commercial acumen” and provides “excellent, practical, business-savvy advice.”
Legal 500, 2019

Key contacts
Philip Nolan
Partner, Head of Technology
+353 1 614 5078
pnolan@mhc.ie

Oisin Tobin
Partner, Technology,
Head of San Francisco Office
+1 415 655 6841
otobin@mhc.ie