The Data Protection Regulation: A Triumph of Pragmatism over Principle?

Simon Davies*

In April 2016, the European Parliament adopted the long-awaited General Data Protection Regulation (GDPR).¹ This instrument was intended to establish a modernised consumer-focused toolkit for privacy protection across Europe – one that is more relevant, effective and harmonised. A core aim was to enhance the digital single market through the creation of certainty of rules across the Union.

What has emerged is a framework that maintains the basis of data protection and adds additional protections, but which falls short of its original promise. While establishing some important innovations, the GDPR could never be described as a ground-breaking instrument for 21st Century protection of rights.

Little wonder. The GDPR’s tortuous passage over four years had been accompanied by aggressive lobbying by corporate interests and by a sometimes intransigent EU Council. Dogged by hostility and stalling tactics, the initiative often ran into trouble. At times throughout its gestation, there was a real risk that the process might collapse.

The proposals were construed by industry – particularly US interests - as controversial and foolish. At one extreme was a claim that the proposed provisions were unrealistic, prescriptive and would harm economic growth and innovation. On another extreme there was (and continues to be in some circles) a fatalistic belief among some companies and entrepreneurs that any international regulation in an era of globalisation, cloud and ubiquitous computing is doomed to failure (that is, ironically, unless the focus of regulation is the protection of their intellectual property rights).

Nevertheless, the proposed framework that finally emerged contains some important safeguards that could improve privacy protection in the years to come. In spite of genuine reservations about precisely how these reforms will be enforced - and by whom - the Regulation provides a more robust data protection infrastructure than its predecessor. There is now a much higher standard required of controllers and processors, greater accountability and transparency and a wide spectrum of reporting requirements. Whether, however, the GDPR provides an adequate enough foundation for longer-term data protection rights is yet to be seen.

---

* Simon Davies has worked in the fields of privacy and data protection since 1987. He is the founder of the watchdog organisation Privacy International.

In some respects, the Regulation is the *Art of the Possible* – offering huge potential but lacking the detailed mechanisms that could make it work. Its implementation – once seen as anathema to innovation and profit – is now being embraced without equivocation by most parties. Without wanting to appear dramatic, data protection dynamics in 2016 are similar to the dynamics of industry after the end of the Second World War. The focus of government and industry shifts rapidly from a war footing to embracing reconstruction and reconciliation.

Nonetheless, the GDPR is marked by posturing, hypocrisy and opportunism. Law firms that once advised clients how to lobby against the initiative, are now excitedly promoting the very benefits that civil society had been promulgating from the outset. US companies that once invested millions of dollars to destabilise the initiative are now telling customers that the Regulation’s logic is impeccable. And of course the European Commission - in spite of the blatant absence of harmonisation in the instrument - promotes it as the very basis of harmonisation.²

**The Positive Elements**

There have, however, been a number of clear wins for data protection rights. One of the most significant of these is the enforcement process. Originally, the European Commission intended to create a ‘One Stop Shop’ mechanism that would allow companies to ‘simplify’ their dealings with data protection regulators by only needing to interact with a single Data Protection Authority (DPA). Widespread concern was expressed that this arrangement would work against the interests of citizens and in favour of large entities. The GDPR now specifies a ‘lead’ Authority for investigations, but it also allow for intervention by other ‘concerned’ regulators. This mechanism could potentially act as a brake on DPAs that are unwilling to take assertive action and it could also provide support for DPAs that are under-resourced. Importantly, these intervening DPAs can refer a decision by the lead Authority to the newly created European Data Protection Board (EDPB).

There is no question that organisations processing personal information are now on notice that they must lift their game. There appears to be consensus – even in Silicon Valley - that use of personal data requires a higher level of due diligence than in the past. Controllers and processors (both of which are now equally liable) need to think carefully about what data they have, where it is located and whose eyes are on it. In essence, this requires a more scrupulous audit and some clear thinking about risk. In many respects, this environment ushers a more systematic approach to handling information.

One extremely important element of the Regulation is that clarity has now been achieved on the question of processing obligations outside EU territory. Organisations

---

handling a wide spectrum of personal data are now under an obligation to conform to data protection and security standards as if they were based on European turf. This may mean, for example, appointing a representative in Europe. The new rules require certain impositions such as the completion of Data Protection Impact Assessments (DPIAs) for risky or sensitive processing.

The GDPR is clear that controllers must only engage with processors who can provide ‘sufficient guarantees’. This requires data owners to check that they have effective ‘technical and organisational measures to ensure the security of the processing’. This element is a clear step forward for data protection.

There have been unexpected wins in the new Regulation. The principle of the Right to be Forgotten has been enshrined, though some argue that this right is poorly conceived in the GDPR.

The potential to also impose substantial fines on offenders is to be welcomed. It is possible now, in theory, for regulators to penalise an organisation up to €20 million or 4% of its annual turnover, whichever is the greater. For a serial offender such as Google\(^3\) this could mean risking a fine of up to €3 billion – higher than even the most aggressive competition penalties. It is, however, debatable whether some DPAs will ever impose such penalties. The UK Information Commissioner’s Office (ICO), for example, was given authority several years ago to impose fines of up to half a million pounds but it chose instead to pursue a ‘light regulatory touch’ with offenders. In 2015 the ICO handed out a total of only £2 million in fines.\(^4\) This approach is in sharp contrast to the US Federal Trade Commission (FTC) which in 2012 imposed a $22.5 million fine over a single action by Google to undermine the privacy of its Safari browser users.\(^5\)

The GDPR has also established a number of other conditions, such as data protection Impact Assessments for particularly sensitive processing operations and a requirement for the appointment of Data Protection Officers (though this would apply only rarely to Europe’s 23 million small and medium sized enterprises).

This shortcoming does not apply, however, to data breaches. The Regulation imposes a universal 72-hour notice period for the reporting of breaches. While this window has been criticised by some commercial organisations as unreasonable, the reality is that national DPAs are likely to show leniency in situations where an organisation could not possibly have been aware earlier of the breach.

---


Given the overwhelming lobbying effort by the industry, it is no surprise that the Regulation continues to protect the legitimate interests of companies to process non-sensitive personal data. However, unlike the Directive, the Regulation’s recitals are very clear about the need to reflect the reasonable expectations of the individual at the time of collecting data. The prevailing view of data protection lawyers is that, in practice, this condition will work in favour of the data subjects’ interests.

The so-called ‘Big Data’ industry may also be affected by the GDPR. This is one of several burgeoning processing sectors which has been taken into account by lawmakers involved in the Regulation. The purpose limitation principle remains intact and is bolstered by specific limitations on profiling. However, as outlined below, there are several important carve-outs and inconsistencies that weaken these protections.

Finally, it is important to recognise the issue of consent, which over the past several decades fell victim to rhetoric and bad practice. The absence of definition and clarity has resulted in a regime of ‘implied’ consent that compromised the very basis of data protection. The Regulation establishes a more robust framework to better ensure that consent in most cases must be explicit. One risk, of course, is that the mechanism to ensure consent could end up similar to the much-lambasted EU cookie notice policy.

As with the Directive, the GDPR stipulates that consent should be ‘freely given,’ and stipulates that consent may not be coerced, for instance by making consent for non-essential processing a precondition to entering into an agreement, or where there is a clear imbalance between the controller and the data subject. The concept of ‘clear imbalance’ is heartening, and it will provide heated debate for many years to come.

A Shaky Edifice Built on an Uncertain Foundation?

Since 1995, Europe has relied on a data protection framework that required all member countries to enforce citizen rights through national law. But even by 2010, that original arrangement was seen by some as archaic and not fit for purpose in the modern age. A new draft regulation was submitted in early 2012 by the European Commission for consideration by the European Parliament.

When the 1995 EU Data Protection Directive was created, each Member State was required to transpose that instrument into its own national law. What transpired were some fairly stark differences in the way each state regulates and enforces data protection. At one level this is a hugely confusing situation both for business and for consumers.

---

True, each nation has its own DPA, but there is little consistency in the powers, functions and limitations of each one. What binds them is a set of principles (proportionality, fairness etc). Add to that decades of legal evolution and you end up with 28 national regulators with wildly different approaches to data protection enforcement. This divergence applies not just in law, but also to the modus operandi and dynamics of each DPA.

In broad terms, for example, Germany and the Scandinavian and Nordic countries enjoy a wide degree of power and autonomy while Ireland has built a more relaxed business-facing culture. The German States (Länder) of Schleswig-Holstein and Berlin often exhibit progressive and technically aware enforcement policies while smaller regulators such as that of Slovakia can barely keep up with day-to-day responsibilities. Some, such as Denmark, tend to be inward-looking. There is a disproportionate load on such countries as Spain and France to take on major issues such as global cloud services.

In some respects, any Regulation is only as effective as the authorities that enforce it. The twist in the GDPR’s fate is that many of the DPAs remain ill-equipped, under-resourced or unmotivated. There is a depressing parallel with the Telco regulation in the 1980s, which throughout much of Europe fell into disrepute through idleness and compromise among oversight bodies such as the UK’s Ofcom. Many DPAs in the past have been too biased or lazy to conduct meaningful investigations.

The jury is still out on whether DPAs can change for the better. Many suffer serious financial constraints and others are steeped in a history of government control and industry bias. As recently as 2014 the European Court of Justice found the need to rule against the government of Hungary after it had arbitrarily removed its Data Protection Commissioner.

The idea of the original Data Protection Directive was to create a consistently high universal benchmark of data protection that gave a predictable standard of rights across the Union. That, at least, was the theory. In reality, because of this diversity of transposition and enforcement, there emerged a system of regulatory arbitrage across the Member States, with only an informal arrangement to achieve a harmonised approach for consistency of decision-making across the EU (the Article 29 Working Group stepped up to this role after the SWIFT bank scandal). One key aim of the GDPR was to resolve some of these issues. The Regulation was originally intended to obviate the

need for implementing legislation at the national level, and would thus create a harmonised framework.

This aim has failed substantially. Because of the associated controversy and a lack of commitment from the EU Council, the GDPR became a creature of consensus: part Directive and part Regulation. Its recitals provide vast scope for wiggle-room by Member States. And while there will be an overarching EDPB it is questionable whether this body will have the political gravitas to meaningfully influence the course of law in Member States.

Such flexibility is also reflected in several carve-outs in international trade agreements, which permit widespread latitude to circumvent key protections in the GDPR. ¹¹

This flexibility for Member States to set their own rules is reflected throughout the entirety of the data protection spectrum. It includes processing for incompatible purposes, processing of sensitive health data, restrictions on the rights of data subjects, security of processing, limitations on safeguards and derogation for public interest reasons. In each case, individual states may decide for themselves the rules that will apply to the processing and transfer of data. ¹²

The GDPR’s flaws, however, extend much further. The instrument fails in many cases to provide definitions that might have formed a foundation for harmonised rules. Equally, the mandate for automated decision-making and profiling appears – if anything – to be more flexible under the GDPR than in the Directive.

To exemplify just one aspect of the Regulation, a group of experts convened by European Digital Rights (EDRi) assessed that Article 23:

…authorises member states to restrict by law the application of data subject’s rights for purposes of national security, defence, public security, the prevention or investigation of crimes, ‘other important objectives of general public interests’ The application of the exemptions remain largely discretionary and almost entirely in the hands of the Member States. Moreover, under this provision Member States can adopt domestic exemptions that directly impact on the processing of personal data in transnational and online contexts: the provision is not limited to exemptions for the benefit of public authorities only, but can also be used to exempt private-sector controllers (companies from the normal requirements relating to data subject rights, e.g., in relation to online fraud detection by banks. The scope is significantly broader than the equivalent article from the 1995 Directive. ¹³


This latitude will have a substantial bearing on many key elements of the GDPR. Consider the aspect of consent, which is one of the main pillars of data protection rights. True, the GDPR makes a distinction between ‘unambiguous’ and ‘explicit’ consent, but the difference between the two remains unclear. Unambiguous consent must be made by a statement or a ‘clear affirmative action’ by the data subject. But what is the nature of this affirmative action?

One resolution to this question is likely to be a loosely constructed accord among DPAs. This arrangement can, however, be overridden by national law. For example, consent by children using information services can only be valid where the child is 16 or older, unless individual Member States adopt a lower age threshold, down to a minimum of 13. Again, this latitude is likely to cause severe problems for many global services.

In conclusion, the GDPR will most likely result in an improvement for data protection rights. In spite of shortcomings, disappointments and lost opportunities, the instrument should provide a more robust infrastructure of rights protection. It is, however, clear that such evolution is unlikely to happen unless regulators and civil society work to use these new tools to their full capacity.