The GDPR at Two: Expert Perspectives

The EU General Data Protection Regulation is celebrating its second anniversary May 25, 2020. For this special project, we asked leading voices in the data protection and privacy community to reflect about the past, present and future of the GDPR.

The following is the compilation of perspectives from policymakers, practitioners and academics around the world. Each author brings their unique point of view regarding what works well or less well in the regulation. The experts discuss the GDPR's global impact, compliance and accountability, data protection by design, enforcement and consumer sentiments. Together, they create a rich quilt work of impressions and projections about the two years past and many years to come.

Gabriela Zanfir-Fortuna, Future of Privacy Forum, Senior Counsel

A personal account: We have a game-changer

You already know the numbers. How many fines, how small or large they were, how much staff was hired by data protection authorities, how much the EU General Data Protection Regulation enlarged privacy compliance budgets all over the world, how many codes of conduct and certification mechanisms were approved (or not) and so on. When the GDPR turns two, I thought a personal account about its significance would bring more to our community's debate than yet another balance sheet.

I have a special relationship with the GDPR. I've been following it from afar (to be precise, from a town 150 miles west of Bucharest), with the fresh enthusiasm of a researcher, since before it was officially proposed. Our paths actually intertwined later on, when I was in Brussels, and I was working with a group of brilliant colleagues from the European Data Protection Supervisor, magistrally steered by Giovanni Buttarelli, on an alternative GDPR compromise text to inform the ongoing trialogue. But my closest encounters with this regulation in fact happened after I crossed the Atlantic and I witnessed first-hand what I believe is the immeasurable impact it had on one of the most stubborn and unique privacy jurisdictions in the world. So here is my personal GDPR review.

When the European Commission published its Communication on a Comprehensive Approach of Data Protection in the European Union in November 2010, announcing a future sweeping reform of the Data Protection Directive, I was just starting my PhD program at the University of Craiova, in Romania, under a general civil law track. I was also struggling to convince my supervisor that data protection is an actual area of law and that it has to do, in fact, with civil law. Data protection was a virtually unknown and provably unstudied legal topic in my part of Eastern Europe, despite the existence of a law transposing the 1995 Directive. I stumbled upon it during an EU law moot court competition, and it fascinated me ever since. It took a year of methodical, classic analysis of a droit subject if civil tailored on the intricate structure of the right to data protection, and the promise of a future legal framework that will have tremendous impact on the day-to-day life of Europeans and that was meant to strengthen their rights as "data subjects," to finally get the seal of approval for my topic of choice.

The GDPR was tabled by the commission as a legislative proposal in January 2012, enriching my research horizons across the board, by adding new rights, expanding those that already existed and bringing more detailed rules on judicial redress. These were the key issues I was analyzing: the rights of the data subject and their adjudication in civil law. After I defended my thesis at the end of 2013, I was happy to accept a traineeship position with the EDPS in Brussels, transitioning later on into a legal officer job. One of the defining projects during my time in Brussels was working with a team of brilliant colleagues on an alternative text of all GDPR articles, as a compromise among the text versions of the European Parliament, the European Council and the original proposal of the commission. This is how I came to know in detail the twists and turns of the text, the nuances, the underlying ideas and sometimes the contradicting intentions of the three institutions directly involved in legislating. Our effort was aimed at informing the negotiations in the trialogue with an independent voice, acting upon EDPS' official role as adviser of the EU legislator in all matters related to data protection.

During that time in Brussels, we knew the GDPR was going to have a serious impact in the EU. Things would unquestionably change, with data protection being more in the spotlight. All public agencies and organizations across member states would have to appoint a data protection officer, potential fines exponentially grew, an EU agency was created, the European Data Protection Board, putting new energies in motion and possibly being the prototype of a new governance model for common EU policies. But, from where I was standing, we never imagined the GDPR would ignite waves of personal data protection reform across the world, at micro and macro level, and would enter into the general public's attention to the extent it did.

I moved to the U.S. in August 2016, a couple of months after the GDPR finally passed, with its two-year grace period. Organizations here, big and small, that had any sort of business in Europe, fell into a frenzy: "Does the GDPR apply to us?" "Do we have to appoint a DPO?" "Do we have to put up a cookie banner?" "Do we have to enter a data processing agreement?" Everyone was at least doing a data map, finally trying to have a detailed picture of what data they hold, where and why, and performing an initial assessment of GDPR readiness. From manufacturers of agricultural machines and exhaust pipe systems, to hotels and casinos, to universities, as far as I could tell, everyone was paying attention to the GDPR and was getting ready for May 25, 2018 — the day it would finally enter into force. When the GDPR frenzy

overlapped with the Cambridge Analytica scandal, I vividly remember gasping in front of my TV, watching American prime time news programs talking about this new law coming from Europe.

On the big day, two years ago, I was in New Orleans on a personal break. I ended up spending that morning explaining what the GDPR is all about to a group I had just met through a common friend. They had nothing to do with the world of compliance or tech, they had no idea I was in any way close to the matter, but all of them were talking about those emails with "We updated our privacy policy" and about this new GDPR law. Outstanding. Back in Romania, not only that established lawyers finally discovered this field, but even my former neighbors now know about personal data and that there are strict rules in place about who can have them and for what.

Once the frenzy of its entering into force calmed, the profound impact of the GDPR became clearer. When I read the text of the California Consumer Privacy Act for the first time, as adopted in summer 2018, I gasped again. There was wording in there that clearly aligned with the GDPR. The first baseline privacy law in the U.S., finally adopted. Since then, I've been following together with my colleagues from the Future of Privacy Forum the waves of comprehensive or baseline privacy bills, at state and federal level. The GDPR, on top of the Cambridge Analytica scandal, seriously revived the privacy and data protection debate in the U.S., after the effervescent '70s. Boosting the framework of global influence created by its predecessor through international data transfers rules, the GDPR also inspired the adoption of a new general data protection law in Brazil and a privacy bill that is being considered in India.

I am fully aware of the criticism brought to the GDPR and its effectiveness, putting a spotlight on the lack of big fines, on the slow one-stop-shop mechanism or on the fact that we don't see many fundamental changes in business models yet. But even if we look at it adding this lens on top of my account above, the GDPR is still a game-changer. Not only that it became a sort of lingua franca of personal data protection programs and regimes around the world, but it created a shift in the public conscience. It brought data protection issues from the fringe to the spotlight.

Ruth Boardman, Bird & Bird, Partner and International Data Protection Practice Co-Head

Personal data protection and focus going forward

The EU General Data Protection Regulation has been responsible for a significantly increased focus on and protection of personal data.

We see the evidence of this all around us on a daily basis. Publicly, we see the more detailed data protection notices required by Articles 13 and 14, as well as the increased media coverage of stories in which privacy and data protection issues are key. Professionally, we have all worked (very!) hard to review personal data processing activities against the exacting GDPR standards and strengthen privacy programs to ensure compliance going forward. We have also welcomed many new people as data protection and privacy professionals and as new friends and colleagues.

The GDPR has achieved this not just in the European Economic Area, but also on a worldwide basis, with countries from Brazil to Thailand updating their laws and looking to the GDPR as a major point of reference.

With all these (and other) achievements, the GDPR must be regarded as a success. But because there is always room for improvement, I'd like to suggest two birthday wishes for the European Commission to make, when it blows out the candles on the GDPR's second birthday cake.

First, enforcement. The EDPB's contribution to the commission's report on the GDPR shows that data protection authorities are taking enforcement measures. However, there are still relatively few decisions imposing significant sanctions. When data protection professionals advise their commercial colleagues on what is needed to comply with the GDPR, increasingly, businesses push back and point to competitors who are not fully complying and where no sanctions have been imposed. The fact that others are behaving in a particular way does not, of course, mean that the approach is correct. We are seeing increasing volumes of data protection litigation, from small claims by individuals, through to representative actions and group litigation. However, private enforcement by individuals cannot take the place of action by supervisory authorities, and the more time goes by without substantial sanctions being imposed, the more this undermines the credibility of GDPR and the ability of data protection officers and privacy counsel to promote compliance in their organizations.

Second, keep the balance between data protection and innovation under review and be willing to make adjustments. Data protection authorities and legislators often say that there is no need to choose between strong privacy protection and the benefits that new technology can bring — that strong data protection laws engender consumer trust on which new services depend. While this is a rhetorical commonplace — and can sometimes be true — it is not always the case. Often, there are trade-offs; data protection laws can inhibit new services and this is not always to the benefit of individuals. To take one example of this, consumers suffer when they are the victims of identity theft and when payments are fraudulently allocated to them. However, in some member states, it is not possible to provide such services and comply with data protection law[1]. It is important that the commission and member states are alert to areas where data protection is proving overly restrictive so that appropriate adjustments can be made.

Eduardo Ustaran, CIPP/E, Partner, Hogan Lovells

GDPR — Success in progress

The EU General Data Protection Regulation is a law on a mission — a now-or-never chance to regulate the use of data in a truly effective way that is aligned with the relentless evolution of the data economy. This ambitious objective inspired policymakers and legislators to create

[1] Because (in some member states) this would be regarded as an automated indivdiual-decision, would not be regarded as contractually necessary and would not be authorised by an EU or member state law. The services would not be effective if purchasers have a free choice as to whether or not to consent to fraud prevention technology being used.

a legal framework built on the foundations of the European approach to data protection as a fundamental human right governed by strong principles but emphasising the technology-driven pragmatism of our time. Two years on since the coming into effect of the GDPR, the signs are encouraging. The law is well known — although not always well understood — and the GDPR has become a hugely influential point of reference for data regulation worldwide. But as with any long-term project, we must acknowledge that the GDPR is still work in progress.

One of the most ambitious aspects of the GDPR has little to do with compliance obligations or individuals' rights. A radical change brought about by the GDPR is its new system of regulatory supervision. Establishing a single pan-European supervisory authority would have been even more radical but pretty much impossible in today's European Union. So the one-stop-shop idea became a suitable and bold alternative that, after much legislative debate, left the European data protection authorities with a considerable management challenge to overcome. Somewhat unexpectedly, it is working. The level of cooperation among regulators is commendable, and although some areas need a more streamlined approach — binding corporate rules come to mind — regulatory action across the EU is largely respectful of the one-stop-shop mechanism.

The GDPR also introduced the novel concept (at least in Europe) of accountability. This has proven to be as useful and versatile as a Swiss army knife. A myriad of tools — from data protection by design to data protection impact assessments and from data breach notification to the ever-crucial data protection officer — have been deployed to make accountability happen in practice. This is data protection as it is meant to be, putting the onus on those who wish to use personal data rather than relying on individuals to control such use. This also involves an accelerated learning process for all that is still happening.

Perhaps the greatest success of the GDPR so far has been the introduction of the risk-based approach to compliance and regulatory action. Data is all around us, and its protection is a responsibility that needs constant recalibration. A static and prescriptive law would have been incapable of addressing the nuances of the digital economy. Fortunately, the GDPR is not that. The GDPR has flexibility and common sense at its core, and thanks to that, we should regard it as a framework that can adapt to the privacy and cybersecurity needs of our challenging world.

Marit Hansen, Data Protection Commissioner of Land Schleswig-Holstein, Germany

The GDPR — data protection at its best? Time will tell

The objectives of European data protection law have been clear: harmonization, modernization, a high level of data protection for individuals with strengthened data subject rights, and thereby facilitating the free movement of personal data under the conditions laid down in the law. This describes the situation in 1995 when the European Data Protection Directive 95/46/EC was adopted.

What happened? Each member state of the European Union transposed the directive into national law, but this didn't turn out to be a European-wide harmonized solution. And how modern is a law from 1995, the year when the internet started to become an instrument for everybody instead of mainly addressing nerds and specialists? So about 20 years later —

which, in the age of digitization, seems like an eternity — "European Data Protection Law 2.0" was elaborated: the EU General Data Protection Regulation. The objectives remained the same: harmonization (this time for real!), modernization, high level of data protection, strengthened data subject rights, free movement of personal data.

Lawmaking needs consensus. Consensus can be achieved if the law is easy to understand and everybody has grasped all provisions, their implications and potential side effects. Or if the law is rather abstract and a comprehensive understanding is postponed to a later stage, namely when the law has to be applied by supervisory authorities or clarified in court. The GDPR is characterized by the latter attempt: Its wording is quite abstract, and sometimes a provision seems to be made up by a mixture of concepts of different origins — from the European Commission, Council and Parliament.

It is easy to criticize the GDPR or to point out small or bigger deficiencies. In the lengthy and tedious negotiation phase of the lawmaking process, it became clear that not all desires of all contributors could be fulfilled. For a supervisory authority, it is clear that the GDPR has to be taken as is. Obviously, the abstract legal text needs interpretation. But, hey, this hardly comes as a surprise.

What is more, from a European viewpoint, not so many provisions of the GDPR break new ground. Sure, instruments such as the data protection impact assessment, a data protection officer or certification have not been known by all member states. But the general principles have not changed significantly.

What has changed is the awareness of data controllers and data processors that there is something like data protection law and that non-compliance may go hand-in-hand with severe sanctions. Also, more data subjects have understood that they have rights — they are by no means powerless. The courts that rarely had to decide on data protection cases become used to it. A huge business has evolved around legal and technical data protection support.

Granted, some players have not changed their data processing and simply claim that they fulfil the GDPR. Currently, the demands for data protection by design and for data protection by default (Article 25 of the GDPR) predominantly are lacking transposition into practice. Dark patterns in software design trick users into revealing more personal data than necessary. So-called consent is often not informed or freely given. The list of shortcomings is long. Sometimes they are caused by ignorance, sometimes the cherished business model opposes the legal requirements and controllers prefer to exhaust all remedies before amendments are agreed upon.

Some people think the first years of a reform law are similar to teething problems. I prefer the comparison with a choir: First everybody has to do a vocal warm-up, which includes humming and singing through scales, on their own and then together, listening to each other — and finally, after some practice, the choir sings with one voice. You cannot skip the warming-up phase if you aim for high quality. This image is valid for the cooperation of supervisory authorities, in addition to controllers and processors, as well as producers of the products, services and applications when designing their respective data processing systems.

My hopes in the effects of the GDPR for achieving fairness in data processing and safeguarding the rights and freedoms of individuals have not been fulfilled yet. But there a small and even some bigger signs for improvements within and outside Europe where the GDPR has already made a change. With the Data Protection Directive, this clearly hadn't been achievable. With the GDPR and further specification of its requirements, as well as provision of best practices, we have a strong chance for the necessary evolution toward fair data processing.

Stephen Wong, Hong Kong Privacy Commissioner for Personal Data

GDPR's second birthday — what does it bring to us?

The implementation of the EU General Data Protection Regulation has surely brought a sea of changes to the data privacy landscape, not just in Europe, but also around the world. Two years on, it is not an exaggeration to say that the impact of the GDPR is being felt everyday far and wide, from industry regulators to the business sector, data controllers and data processors to individual data subjects. It was indeed a trendsetter and catalyst for change, given its updated data protection conventionally and the explicit compliance requirements on the part of the organizations established outside EU in specific circumstances. As a regulator from the Asia-Pacific region with close economic and business ties with Europe, it is my distinct privilege to share my initial thoughts on the operation of the GDPR on its second birthday.

It is trite that technology neutral legislation allows for the possibility of legal statutes to cope with information and communications technology development in a dynamic manner. While it is often said that laws always lag behind technological development, the rapid pace of innovation in our day and age makes most related legislation stale in little time. As a landmark piece of legal instrument, the GDPR's technology neutral approach keeps the regulatory requirements constantly up to date without the need for frequent reviews. In addition, the adoption of risk-based approach in data protection is another key to the effective implementation of the GDPR. The approach determines the level of data protection through an assessment of potential harm, allowing data controllers to proactively manage the risks involved with their business operations. This pragmatic approach is well poised to be welcome by the business community.

That said, the changes to the privacy landscape brought about by the GDPR cannot be underestimated. Since its introduction, the GDPR has flagged up awareness and understanding of protecting and respecting personal data privacy right with penalties that should serve as effective deference to any noncompliance. In this regard, the GDPR is very successful in returning control of personal data to individuals or data subjects as part of their inalienable human rights. It also results in a lot of companies building in privacy accountability as part of their corporate governance strategy, an achievement that should definitely be applauded.

At the first glance, the GDPR is wide encompassing, perhaps at least from the eyes of those outside Europe. However, the GDPR also sets a benchmark for the world, almost like a golden standard that other legislation should consider meeting. It is not a coincidence that more and more similar laws and regulation are being enacted around the globe nowadays. For example, in the West, we have the California Consumer Privacy Act, coming into effect Jan. 1. In the East, the India Draft Data Privacy Bill is pending Parliament's approval. Hong Kong is also

in the process of reviewing its Personal Data (Privacy) Ordinance by making references to GDPR standards and guiding principles. This is a welcoming improvement as it tends to reduce fragmentation of legal requirements cross-nationally, though the issue of interoperability is another step to go forward.

Technology evolves every day, and so will data protection frameworks. The GDPR is definitely not the end of our journey but a very firmly grounded starting point. It may, however, not be taken as a straitjacket as small and medium enterprises with less resources could find compliance too challenging. Of course, from the perspective of a regulator, it is imperative for every entity to be treated equally before the law, regardless of their size or resourcefulness. It might fall on us as regulators to engage the SMEs with more guidance, advice and incentives for their compliance readiness.

Lee Bygrave, Professor of Law, Director of the Norwegian Research Center for Computers and Law, University of Oslo

The Byzantine Turn in EU Data Protection Law

EU data protection law — with the EU General Data Protection Regulation in the "front seat" — has taken what I call a "Byzantine turn." By this, I mean three trends. First, the EU data protection system has become an empire in itself and unto itself. Consider its mammoth number of rules, immense officialdom, constitutional standing and strengthened sanctions regime, combined with high-profile judicial support for its cause — all these factors combined give the system the pondus of "empire." With that pondus there comes a certain swagger that bespeaks the following message to the world: "I am now so big that I don't need to justify my being. I am what I am and I am here to stay, regardless of what you might think." It is not difficult to read this sort of message into the subtext of the GDPR or into the subtext of some of the Court of Justice of the European Union's landmark judgments in this field (e.g., its judgment in "Schrems I"). Of course, such a message is far from unique for EU data protection law; numerous other laws, especially those embodying a nation state's ordre public convey a similar message.

The second dimension to the Byzantine turn is the evermore self-referential thrust of the EU data protection system. It is a system increasingly turned in on itself. Large parts of it are essentially engaged in a conversation with other parts of it. The GDPR exemplifies this well. Many of its provisions are addressed not really to the world-at-large, but also to "insiders." For instance, over one-quarter of the words making up the GDPR's operative provisions are devoted to the workings of supervisory authorities and the European Data Protection Board. At the same time, general discourse on data protection has become extremely GDPR-centric; the regulation has effectively created a vortex that sucks policy discussion into its fold. This is occurring not just in Europe, but also across the globe.

The third aspect of the Byzantine turn concerns the procedural intricacy of the EU data protection regime. Data protection law in general has always had a predominantly procedural thrust. Under the GDPR, however, procedural intricacy has become extreme — and extremely problematic. The GDPR's provisions on the "consistency mechanism" are a case in point. It is often said that the "devil is in the detail," yet excess of detail is in itself a devil. It becomes even more devilish when the detail is set out in cumbersome, dense and arcane prose.

All up, the EU data protection system has become a huge sprawling structure — a Kafkaesque castle full of semantic mazes, winding procedural alleys, subterranean cross-passages and conceptual echo chambers.

I appreciate that the GDPR has to be more exhaustive than the directive it replaced if it is to ensure greater pan-European uniformity of rules. Yet, there are costs in trying to leave no stone unturned, just as there is a point where the perfect becomes the enemy of the good. And I believe that the GDPR would be considerably more "user friendly" if at least some of its extremely procedural parts along with those parts that otherwise address the organizational mechanics of supervisory authorities and the EDPB were taken out and put into a separate instrument. The remainder of the GDPR would then address the world-at-large and set out the core principles, rights, duties and sanctions as they concern data subjects, controllers and processors. This pruning would leave the GDPR more digestible and more neatly packaged than its current state.

Lokke Moerel, Tilburg University, Professor, Global ICT Law

EU data protection laws are flawed — they undermine the very autonomy of the individuals they set out to protect

The European Union is supposed to have the strongest data protection laws in the world. So why do privacy violations continue to make the headlines? I believe that the lack of material privacy compliance is not due to lack of enforcement but to a fundamental flaw in our European data protection laws. Our laws are supposed to ensure people's autonomy by providing choices about how their data is collected and used. In a world driven by artificial intelligence we, however, can no longer understand what is happening to our data and the concept of free choice is undermined by the very technology our laws aim to protect us against. The underlying logic of data processing operations and the purposes for which they are used have now become so complex that they can only be described by means of intricate privacy policies that are simply not comprehensible to the average citizen. Further, the reality is that organizations find inscrutable ways of meeting information and consent requirements in a way that discourages individuals from specifying their true preferences and, therefore, often simply feel forced to click "OK" to obtain access to services.

Our data protection laws have resulted in what Professor Corien Prins and I have coined "mechanical proceduralism" (read here), whereby organizations go through the mechanics of notice and consent without any reflection on whether the relevant use of data is legitimate in the first place. In other words, the current preoccupation with what is legal is distracting us from asking what is legitimate to do with data. We even see this reflected in the highest EU court having to decide whether a pre-ticked box constitutes consent (surprise: it does not). Privacy legislation needs to regain its role of determining what is and what is not permissible. Instead of a legal system based on consent, we need to rethink the social contract for our digital society by having the difficult discussion around where the red lines for data use should lie rather than passing the responsibility for a fair digital society to individuals to make choices they cannot fully comprehend.

What does this mean in practical terms when it comes to General Data Protection Regulation? It means that privacy protection is for now best served by adopting the legitimate interest ground as the only legal basis for data processing (read more on these proposals here and here). Any processing of data is contextual, and having been a practicing lawyer even before the Privacy Directive came into force, my conclusion is that any attempt to regulate specific processing activities upfront will be counterproductive, because the issues at hand will either be over- or under-regulated. The European Data Protection Board does an admirable job of trying to mitigate any such issues, but the end result is that this makes the GDPR unnecessarily complicated to apply for businesses, which ultimately undermines its effectiveness and legitimacy. Here are two examples to further clarify my point.

The regime for special categories and criminal data (Articles 9–10 of the GDPR)

The debate about which categories of data should qualify as "special" has become irrelevant. Practice shows that the same data may be sensitive in one context but not in another. Rather, the use of data may be sensitive. As a consequence, the existing regime — which is based on the processing of a predefined set of special categories of data — does not achieve the intended effect. It sometimes over- and sometimes under-regulates (see for examples my IAPP op-ed on special categories of data and IAPP op-ed on GDPR drafting flaws. These issues are already well-known to the EDPB (and its predecessor, the Article 29 Working Party) and have been addressed in their opinions by introducing additional requirements. For example, the specific legal grounds of Article 9 of the GDPR do not require a contextual balancing of interests, which would include an assessment of the measures taken by the controller to mitigate any adverse effects on the privacy of the individuals concerned. In this respect, the legitimate interest ground, contrary to what is often thought, actually provides greater privacy protection for individuals (see also the WP29 Opinion 06/2014, pp. 9–10). The WP29 had already attempted to overcome this problem by requiring that the protection of such data under Article 9 of the GDPR should not be less than if the processing had been based on Article 6 of the GDPR and subsequently applying the legitimate interest test on top of the regime for special categories of data (Opinion 06/2014, pp. 15–16). This begs the question: Why not apply the regular grounds of Article 6 in the first place (which work fully well for other types of sensitive data, such as genetic data, biometric data, location data and communication data)?

Automated decision-making, including profiling (Article 22 of the GDPR)

Article 22 of the GDPR applies solely to automated decision-making and, therefore, does not apply as long as the output of an algorithm is subject to meaningful human review (see WP29 Opinion on Automated Decision-making and Profiling, p. 20). However, in practice, we see many examples of artificial intelligence–assisted decision-making whereby algorithm output is indeed reviewed by a human, but where the output itself may well be wrong, not explainable or biased, as a result of which the subsequent human review may obviously also be flawed. The U.K. Information Commissioner's Office recently issued draft guidelines on explaining AI, basically applying the same requirements also to AI-assisted decision-making, not on the basis of Article 22 of the GDPR, but on the basis of the general GDPR principles of fairness, transparency and accountability (see Part 1, p. 10–11). I wholeheartedly agree with this position, but it again begs the question of why we would need the narrowly written Article 22 of the GDPR in the first place. It puts organizations very much on the wrong track when deploying algorithms, which will lead to noncompliance and potentially unnecessary litigation.

My proposal is to delete Article 22 of the GDPR altogether. The EDPB can then provide guidance on how to apply the legitimate interest test and the general principles of the GDPR to automated profiling (read more). If this is too shocking an approach, I recommend to at least turn around the scope of Article 22 of the GDPR: instead of applying to "automated decision-making, including profiling," the provision should apply to "automated profiling, including AI or AI-assisted decision-making."

Bojana Bellamy, CIPP/E, President, Centre for Information Policy Leadership

The positives, the challenges, the unfulfilled promises

It is fair to say there has not been another single EU law that has had such a profound global impact like the EU General Data Protection Regulation — impact on organizations across the globe figuring out how to comply with it, impact on governments reflecting on it (to a greater or lesser extent) when crafting their own national laws, impact on data engineers and entrepreneurs attempting to code fair processing into their artificial intelligence models, impact on data protection authorities stepping up to their more sophisticated role as data regulators of the digital economy, and impact on people feeling reassured by "the knight in shining armour" to protect their fundamental right to data protection.

On the business and compliance front, the GDPR has brought tangible benefits. It enabled a dynamic shift in organizational approaches to data protection. Data privacy rose from the backroom to the boardroom — and not only for the fear of a 4%-of-annual-turnover fine. But because it became firmly linked to the organization's data strategy and digital transformation. The GDPR instilled good data management and hygiene, enabling organizations to know, care and protect their data and use it responsibly. It actually impacted the business bottom line, by creating a positive return on the investment in accountability — a data privacy management program. More granularly, the GDPR's risk-based approach compelled organizations to foster a consistent discipline of assessing data privacy risks. It also forced organizations to deliver more user-centric transparency to individuals and build effective processes for responding to individuals exercising their data privacy rights.

These efforts resulted in greater data protection for individuals and much-needed trust in the fourth industrial revolution that we are all living through. Individuals, business partners and investors expect organizations to use data responsibly and offer value for the data deal.

Yet, the GDPR is not without its challenges. An over-emphasis on consent has diminished the real value of other grounds for processing, such as legitimate interest, and is weakening the value of consent itself. Several GDPR provisions are leading to tensions with emerging technologies, including AI and machine learning, biotechnology and blockchain. And DPAs are facing regulatory burdens. They are buried under an avalanche of complaints, breach notifications and populists' calls for enforcement, instead of building engagement and leading from the front. The GDPR has dealt them a tough hand — complex procedures to work together and even unrealistic tasks and expectations within their current means and resources.

Finally, maybe it is the unfulfilled promises that the GDPR romantics among us regret most — certifications and codes of conduct, using the one-stop shop and consistency beyond just enforcement, full harmonization of the rules, consistent and risk-based interpretation of the GDPR from regulators, and finally, harnessing the full potential of organizational accountability.

I am optimistic and believe we can overcome the challenges and realize those valuable promises. This will require deep and novel thinking; courage to break away from conventional interpretation, innovation in the way we deliver regulatory oversight and encourage the "race to the top," and leadership to consider data privacy as a business value, enabler and driver of digital trust and growth. Companies, regulators and policymakers have no time to waste and must act now. Otherwise, the benefits of the fourth industrial revolution and the opportunity to deal with the challenges it presents will slip away.

Peter Swire, Alston & Bird, Senior Counsel

Risks to data transfers from the EU to the rest of the world

As the EU General Data Protection Regulation turns two, there is a difficult issue that, if not resolved thoughtfully, could lead to prohibiting transfers of personal data to most countries outside of Europe. The issue concerns this current doctrine of the Court of Justice of the European Union: What constitutes "essential equivalence" under the GDPR for the safeguards that apply to foreign governments when they access personal data for law enforcement and intelligence purposes?

European law, to assure protection of personal data when sent to third countries, may have backed itself into a corner. I reach this conclusion reluctantly, after many years of working to ensure stronger safeguards against over-reaching government surveillance. The first Schrems case struck down Safe Harbor, based significantly on the (incorrect) view that the U.S. National Security Agency had "unrestricted access to mass data." The Irish court hearing the second Schrems case faulted the judicial and other safeguards that exist under U.S. law against improper surveillance, despite extensive and often-unrebutted evidence to the contrary. That case, although not yet decided by the CJEU, may well strike down the lawfulness of many transfers under standard contractual clauses or call into question the Privacy Shield.

To make the issue more concrete, imagine a controller in the EU who wishes to transfer employee or customer data to a third country, such as China or the United States. Today, the controller most often uses SCCs, authorized by Article 46 of the GDPR. Under Article 46, the controller has the responsibility to apply "appropriate safeguards." The difficulty, however, comes when a European court or data protection authority also assesses the rules and procedures used by the foreign government for court orders and other mandatory actions taken within that country. As I have written elsewhere, if the U.S. fails the test, then China and most other nations globally also deserve to fail. The issue becomes even more acute with Brexit, given the criticisms the U.K. has received concerning its rules for government access to personal data.

Here are three possible outcomes:

1. **More flexibility in determining "essential equivalence."** Under this approach, the EU would provide greater flexibility concerning a government's access to personal data within its country. Within Europe, the European Court of Human Rights has long permitted governments a "margin of appreciation" in how they reconcile national security and public safety, on the one hand, with fundamental rights to privacy. More broadly, international law for centuries has deployed the concept of "comity," which essentially is a measure of deference to other nations' differences. This approach would enable transfers of personal data to democracies, such as the U.K., the U.S., and others, with a greater permitted margin of difference than the current doctrine of "essential equivalence" would seem to allow.

2. **No EU review of third country access to personal data.** The first approach would enable data transfers to countries with a strong rule of law. It would not, however, seem to provide any basis to transfer data to countries such as China that lack basic protections against government access to personal data. If the EU wishes to continue trade with China, then it would appear to need a new legal approach concerning government access to personal data. I have asked a number of leading EU data protection experts but have not found any proposal for such an approach. One legal change to the GDPR could be to say that controllers would need to take appropriate protections within their control, but would not be bound under SCCs to refuse mandatory requests from third country governments. This approach would enable continued trade between the EU and China, although it would be less protective of fundamental rights than the first option.

3. **No change to GDPR.** If there is no change to the essential equivalence doctrine, then transfers to the U.S. under SCCs may be found unlawful. Transfers to China and many other countries would seem even more clearly unlawful due to the lack of protections against government access to personal data.

Any changes could be made to Chapter V of the GDPR governing transfers of personal data to third countries. Without any such change, the lawful basis will be shaky at best, with significant consequences for commerce.

Sophie Kwasny, Council of Europe, Data Protection Unit Head

Shining like gold

Our dearly remembered Giovanni Buttarelli wrote April 1, 2016, in a paper titled "The (EU General Data Protection Regulation) as a clarion call for a new global digital gold standard" that "the GDPR is going to raise the bar for data protection laws around the world."

We are now four years after the adoption of the text, and nearly two years after the start of its enforceability, what happened around the world during those two years? We notice at global level an abundance of new data protection legislations, with more than 10 laws adopted in 2019 on several continents and in 2018, multiple upgrades of existing legislations, such as in Israel, New-Zealand and many EU countries obviously, as well as completely new laws in Brazil and the state of California in the U.S., for instance.

2018 was also the year when the modernized Convention 108 was adopted. The EU sees it as reflecting "the same principles as those enshrined in the new EU data protection rules and thus contribut[ing] to the convergence towards a set of high data protection standards" and as a "plus" for countries seeking an adequacy recognition (see Recital 105 of the GDPR).

It is interesting to examine how much of an influence the GDPR has had on those legislative developments. For the modernization of Convention 108, consistency between both legal frameworks was essential for all EU member states (as they are all also bound by the Convention). For national legislations around the world, the level of GDPR intake seems to vary, some laws being close to a copy-paste, while others maintain strong national perspectives and specificities (see some African and Central Asian laws enacted in 2019, for instance).

It is obvious that countries around the world are responding to a fast-changing digital environment and the economic prospects attached to it. They want to protect individuals from the multiple threats arising in the context of the processing of personal data and to facilitate transborder data flows. They want to harvest the digital potential, and they want it fast. But this journey, the journey to strong enforceable data subjects' rights, to accountability, to safeguarding human dignity in an age of algorithmic decision-making is not a journey with shortcuts.

Buttarelli concluded his 2016 paper expressing the hope that "during the period of a generation for which the GDPR is likely to apply, we will have achieved a common standard, a sort of digital gold standard [...]".

My hope is that to achieve that common standard, countries around the world will realize the uniqueness and value of Convention 108+, its committee and the global cooperation forum it offers. On their route to that gold standard, the Convention and its committee are there for them to exchange, learn, try, correct, grow, and finally achieve a high-level global understanding and practice of data protection as a fundamental need in our digital era.

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia Faculty of Law, Founding Co-Director & Senior Researcher, Australasian Legal Information Institute (AustLII)

Evaluating GDPR: Global impact on surveillance practices

An evaluation of the EU General Data Protection Regulation's first two years depends upon how you measure "success," which means you must ask what you hope it can achieve. I want the GDPR to make a substantial contribution to the dismantling of surveillance capitalism and its replacement by a less dangerous information-based capitalism. A European data privacy law cannot achieve this goal by itself, no matter how strong its principles or its enforcement. Fundamental changes to the business models of surveillance capitalism will at least require the parallel efforts of EU competition, consumer protection and anti-discrimination laws, and regulators. It will also require complementary contributions by data privacy and other regulators and laws globally, not least in the U.S., which is the home and "safe harbor" of the inventors and key proponents of its practices. Seen from this perspective, how does the GDPR shape up as a 2-year-old toddler?

The GDPR's first great success has been as a global inspiration for legislation that borrows from its principles and enforcement mechanisms. For 50 years since Hesse's "Datenschutzgesetz" of 1970, countries have been slowly enacting and even more slowly enforcing data privacy laws. As of December 2019, 142 countries have done so. These laws are of greatly varying quality but overwhelmingly influenced by the European model of data privacy laws. Since 2016, new laws outside Europe have included hundreds of examples of GDPR-inspired principles or enforcement mechanisms. In Asia alone, new laws in Thailand and Korea and bills in India, Indonesia and Sri Lanka are creating a new post-GDPR momentum. In Africa, 14 countries have new laws since 2014. The new global template is becoming a version of the GDPR.

Competitors for global influence are unimpressive. Asia-Pacific Economic Cooperation Cross-Border Privacy Rules, designed to hoover the world's personal data into the U.S., is deservedly dead — only 28 US companies and 3 Japanese companies, and no others, participate after a decade. The Organisation for Economic Co-operation and Development privacy guidelines are stuck in 1980, unwilling to go forward.

Within the EU, administrative fines necessarily move slowly through the GDPR systems, due to rights of appeal and the consistency mechanism's collaboration requirements among data protection authorities. So far, the highest proposed fines (not yet finalized) only amount to less than $250 million (British Airways), but they are capable of being in the billions and need to be. Meanwhile, lesser fines establish precedents for breaches of key GDPR provisions, such as Google's $8 million fine by Sweden's DPA for delisting (right to be forgotten) breaches. Enforcement actions initiated by data subjects or their representatives are well-supported and required by the GDPR (Article 80). Many of the most significant GDPR enforcement actions have been at the initiative of "privacy NGOs," such as NOYB and LQDN. So far, nongovernmental organization–supported actions have focussed on obtaining corrective actions and administrative fines, but they will soon also include large-scale actions for compensation (Article 82). Depending on national laws, class-actions involving commercial lawyers will also emerge. Shutting down infringing types of processing will depend on national laws (Article 84). The GDPR has all the tools to create a market for privacy enforcement, a level of "responsive regulation" Europe has not previously seen. Will EU regulators be willing to use them to their full "dissuasive" effect, and will EU courts endorse their approach?

The long-term success of the GDPR also depends on its perceived effectiveness in imposing reasonable restraints on EU governments, not only on businesses. A significant threat to the GDPR comes from COVID-19 and state surveillance. The European Data Protection Board has stated that data protection rules, including both the GDPR and the ePrivacy Directive, do not hinder measures to fight a pandemic. They point to various legitimate grounds for processing and exceptions but stress that restrictions must be "proportionate and limited to the emergency period." COVID-19 is a daunting test of these requirements for GDPR credibility as a global standard.