Position Paper on

Fixing the GDPR: Towards Version 2.0

25 May 2021

The promises of the General Data Protection Regulation (GDPR) are manifold. It is supposed to protect privacy and guarantee the self-determination of the individual. It is supposed to put digital gatekeepers in their place. It is supposed to be a bulwark against the surveillance state and surveillance capitalism. The law is - for its advocates - the new gold standard for data protection. If you are trying to make an honest assessment of the GDPR three years after its application, you will however also hear very different views. Many citizens, research institutes, charitable organizations and small companies strongly complain about yet another EU bureaucracy monster that overcomplicates their daily lives and massively increases their expenses, being out of all proportion in terms of a cost-benefit ratio. Moreover, you will notice well-founded criticism based on fundamental rights, claiming the GDPR to have a detrimental effect on civil liberties and to undermine important standards of the rule of law.

When I wrote the 2011 own-initiative report for a *'Comprehensive approach on personal data protection in the EU'* (that resulted in the subsequent GDPR) as Rapporteur of the European Parliament, I was a strong proponent for legislative action. Alarmed by constant data protection scandals, I saw it as our democratic duty to harmonize the fragmented national systems and to strengthen our citizens' right to privacy substantially. In this sense, I would still consider the GDPR a success. However, already during the political negotiations on the GDPR as Shadow Rapporteur, I realized that the law also has numerous shortcomings. Over time, I became more and more critical towards those points and eventually, most of my criticism was confirmed in the public outcry after the GDPR's application in 2018. The European Union did create a law that might be excellent in theory and which did improve the standards for data protection in many areas. Yet, it has also caused legal and practical chaos in other areas.

No matter how good the intentions of the legislators are, their laws will never be perfect. Miscalculations are part of policy-making and we are responsible for fixing them. What shocked me was therefore the reactions of certain decision-makers in Brussels and of data protection authorities, which are disregarding the public outcry until today and which are still unwilling to acknowledge that problems exist. To them, the GDPR is "the perfect law" or even "the privacy bible". To them, existing problems are solely the fault of the Member States that wrongly implement the law; of our companies and citizens, who do not understand it correctly; of the legal advisors, who do not explain it properly; of the supervisory authorities, who do not enforce it properly; and of the opponents of the law, who deliberately create confusion.

After hearing the same line of argumentation again in the LIBE-committee earlier this year, when I was negotiating the new GDPR-resolution as Shadow Rapporteur, I decided to try something new. On 16 February 2021, I launched my own public consultation to hear your thoughts about the GDPR. With more than 180 replies, you reinforced my doubts and described how the GDPR is leading to numerous problems in your daily life. Striking was that only 1/3 of the replies was coming from companies and business associations, while the large majority was from citizens, researchers, scientists, nurses, data protection officers, lawyers, non-profit associations, sport clubs and many more. The following list categorizes and summarizes your feedback.

While this list concentrates solely on conceptual flaws, legal gaps and practical problems that occurred since the GDPR became effective in 2018, this document does not argue that the law itself should be withdrawn or that its adoption was per se a mistake. Data protection is and must always remain an essential element of our democratic system. Moreover, the GDPR stands for a major improvement of the right to privacy. Neither I nor other critics want to lower the EU's high data protection standards. However, what the list is clearly demonstrating is that the law, in its current form, at the same time abridges other fundamental rights, leads to a compliance costs explosion and severely hampers Europe's digital transformation. We owe it to our citizens to acknowledge these facts and to start fixing the GDPR-related problems through legal adjustments as well as better guidance. What we need is a new mindset when it comes to the use of data. In our digital world, data offers various chances to improve the living standards and to address current problems such as climate change or a pandemic. Only at the second step, we should focus on the risks and build up effective safeguards to prevent potential misuse. Digitalization is a huge chance for the EU. Let us start by making the GDPR a more balanced law.

Contents

I. Conceptual flaws of the GDPR

'One-size-fits-all' approach

The law does not differentiate between different companies (global corporation /digital gatekeeper vs. local SME/start-up/independent bakery shop) by taking their differing capabilities to comply with data protection rules into account. Furthermore, it does not distinguish between the processing of personal data by private individuals and by state authorities.

Sectoral differences

The law also does not distinguish between different sectors (e.g. health and finances) or different technologies (e.g. AI or Blockchain) and fails to clearly define both. Instead of concentrating on basic and well-designed rules containing clear definitions, principles and methodologies that are supplemented with satellite directives for the different sectors and technologies (= normative specification), the GDPR aspires to protect everything at the same time.

Risk-based approach

Although the concept is covered in general, it is not consistently implemented in the legal text. The GDPR does not differentiate enough between low-risk and high-risk applications, determining - with a few exceptions such as prior consultation of the DPA for high-risk applications - largely the same obligations for each type of data processing. The possibility in the GDPR to define different risk classes of data processing, which require different legal bases, is not being used. Moreover, supervisory authorities are often unwilling to designate low-risk data processing operations as such and thus, prevent the reduction of compliance burdens.

Complexity

The provisions are too numerous, complex and difficult, allowing only a few distinguished experts to really keep track and understand all of the legal consequences.

Outdated concepts

The GDPR uses provisions and approaches from previous legislation, some of them even going back to the 80s. To start with, the law is based on the processing of individual data (thus ignoring Big Data) as well as on the processing by a single controller (thus ignoring cloud computing, the Internet of Things, platforms or other complex actor

networks). The GDPR also assumes that data is processed at a specific location on a fixed hard drive (thus not taking into account that data is no longer stored at a physical resource but instead is globally moving from server to server in global networks, interconnected clouds and blockchains). The principle of purpose limitation excludes chance discoveries in the field of science (e.g. correlations between findings). To sum up, the GDPR does not take into account that current technologies (e.g. AI) function completely differently. The old data protection ideas (e.g. data minimisation) - that the GDPR is based on - are therefore not workable anymore.

Data institutions

The law does not provide the opportunity for trustworthy third-party agents such as data trusts or a new European agency for data to benefit from more flexibility for an agreed purpose. Those institutions could help opening up data silos to SMEs and researchers, facilitating the sharing of confidential and personal data and increasing access to data. The donation of data is also too complicated, if not impossible, under the provisions of the GDPR. Since the Data Governance Act addresses some of these issues, legislative overlaps with the GDPR need to be prevented.

Scope of protection

In contrast to the Data Protection Directive 95/46 that saw the protection of privacy of natural persons as the main interest, the GDPR postulates in Art 1(2) that it protects "fundamental rights and freedoms" of natural persons. However, if the law wants to protect all rights and freedoms, it leads to an excessive demand on controllers, as they would theoretically have to take all fundamental rights and freedoms into account, in all 68 obligations and in all 82 balancing tests of the GDPR. This can never be fulfilled in practice.

Disproportionality with other fundamental rights

The GDPR fails to clarify that data protection is not an absolute fundamental right, but should instead be balanced with other fundamental rights or interest such as the right to life, to liberty and security, the freedom to conduct a business or the freedom of the press. In collision with the standing jurisprudence on Art 8 CFR or Art 16 TFEU, more and more decision-makers and regulators are however supporting this radical interpretation. Besides that, the GDPR does not take into account that the processing of personal data by the controller is, in itself, also protected by fundamental rights (e.g. the freedom of

science or the freedom to conduct a business).

Justification of processing

As every type of processing personal data restricts the right to data protection, each of these restrictions needs a justification based on the law. Justifications may derive from the rights and interests of the controller, from rights and interests of a third party or from public interest. The GDPR, however, does not contain a coherent concept of how and when the data protection right is lawfully limited. The rights and interests that conflict with the data protection right are listed in a rather fragmented and erratic manner. The difficulties during the COVID-19 pandemic have put a spotlight on this issue.

Paradigm change

Data protection laws were initially conceived as the rights of citizens to defend themselves against the state. This approach was changed, though mostly unnoticed. Rules that were only made for the state before are now also applicable to the relationship between citizens and in the relationship between companies and citizens but also between companies themselves. Equating data processing in the public and non-public sectors is highly problematic in legal theory and one of the main reasons for the lack of flexibility in the GDPR.

Prohibition principle

The GDPR sees any processing of personal data as a potential risk and forbids its processing as a principle. It only allows it if a legal ground is fulfilled. Such an anti-processing and anti-sharing approach does not make much sense in our data-driven economy and is contrary to the general objective in Art 1(3) GDPR that promotes the free movement of data. Shifting measures against dangers to a very early stage where the risks are still very abstract also leads to a rule of law problem. An enforcement no longer requires a concrete danger to a sufficiently specific legal asset as is the case in customary police law. Consequently, also the powers of intervention of the data protection authorities go far beyond the normal standards for public authorities. The law as such aims to control the internet and its users as comprehensively as possible. It also wants to establish the view that processing of personal data is generally regarded as a socially undesirable behaviour. This approach is not only latently hostile to progress. The result is that even the processing of personal data that is protected by fundamental rights or that is socially desirable for the protection of public

interest comes under constant pressure to justify itself (e.g. sharing the data of potential recipients of vaccines or the delay of COVID-19 tracing apps).

Overburdening of controllers

The GDPR imposes the controller with numerous duties (e.g. legal base, weighing of interests, obligation to inform and to hold proof, explanation of legal remedy), leading to disproportionate compliance costs that are exceeding the real benefits by far. What seems good in theory leads to situations where obligations are only fulfilled schematically or are even ignored in practice.

Primacy of consent

Although the GDPR has six equally sufficient legal grounds for processing personal data, many data protection authorities and policy-makers see consent as the cornerstone of data protection. Giving the user the illusion of control, the controller is thereby able to pass the responsibility on to the user in complex and page-long data protection declarations. Being on the edge after another privacy banner pops up, many users excessively consent to everything in order to finally get the service they were looking for, often without knowing what they actually agreed to. Such focus on consent has further strengthened the dominant position of a few large companies which, due to their consumer facing position, are at a competitive advantage to collect such consent in a centralized manner for all their services, or as part of their terms and conditions. Subsequently, they can use data collection for innovation and product development at the expense of SMEs or start-ups. In addition, the extreme interpretations of the principle of freely given consent tends to disregard the reality of many data-based business models, having placed such business models in strong legal uncertainty, with consequences for SMEs and for content/services offered to individuals online.

E-privacy regulation

Although the rules laid down in the 2002 Directive governing the confidentiality of communications need an urgent update, the European Commission's plans for a draft regulation as well as the European Parliament's first reading position fail to align the old rules with the GDPR. Instead, they create a separate track of privacy law that would throw the whole EU privacy policy into contention. Content wise, there is no reason why electronic communications data should be regulated outside of the GDPR. Definitions, legal basis and provisions on profiling are already listed there. Why should the GDPR apply to files published on

a website, while the new e-privacy regulation applies if the file is sent via email?

Impact on other laws

Due to the extensive and horizontal legal scope, the GDPR will overlap with and contradict existing and forthcoming laws. The relationship with the Data Governance Act, the Database Directive and the Data Act is particularly worrying. With those packages, the EU pursues the important goal to become a global leader in the data economy. It wants to accelerate data processing as well as sharing. However, the GDPR generally forbids the sharing of private data at the same time, as described above. In reality, this is highly problematic, as the separation of private from non-private data is not always feasible (mixed data) and at least an expensive process. Therefore, data protection rules and the resulting legal uncertainty will lead to lower quality datasets in the European Data Spaces and more reluctance from companies to share data.

Complicated international data flows

Although the GDPR foresees several mechanisms for international data flows (which are critical for European companies with affiliates, customers, vendors or suppliers in third countries), only three of them can effectively be used by entities. As a result, international data flows are currently under threat, which risks isolating the European Union from the rest of the world.

II. Emerging Technologies

Although the GDPR is meant to be technology-neutral, the law and its concepts are not compatible with many new technological developments. With the principles of data minimisation as well as the purpose and storage limitation in Art 5, the GDPR's focus on the processing of individual data by a single controller in Art 4 or the restrictions of the secondary use of data are no longer problem-adequate. Those concepts in fact prevent emerging technologies from exploiting their full potential. Consequently, European companies do not invent as much as they could, stop to develop their prototypes further or even leave the EU altogether as it happens with many start-ups. The legal uncertainty is just too high, even more so since DPAs/EDPB are interpreting many provisions of the GDPR too restrictively. Below, some of the affected technologies and processes:

Artificial Intelligence

In Europe, it is difficult to train algorithms with sufficient levels of personal data (e.g. to enable AI to help with diagnoses or drug development) as vast amounts of high-quality data sets would be required for that purpose. The GDPR provisions on purpose limitation and data minimisation as well as the restrictions on secondary use can be seen as the major obstacles for AI. For instance, purpose limitation requires researchers and companies to get each data subject's permission before doing anything new with their data. This makes consent harder to maintain, and prevents researchers and companies from experimenting with their algorithms, even in cases when repurposing would not affect consumer welfare or privacy. The lack of anonymization procedures and the fact that the training of algorithms is not recognised as statistical or scientific purpose (Recital 162) are further reasons. Finding a legal ground for processing data in case of autonomous behaviour and for complying with the information duties as well as the transparency, accountability and explainability principles of the GDPR is also a decisive challenge for developers and operators of AI-systems. Explainability can be particularly challenging due to all the stakeholders involved in the process of building and using an AI system, as not everyone has a sufficient level of knowledge of the processes involved. As a result, it is unclear what is realistic, feasible and practical when having to provide explainability. When it comes to transparency, externalities such as risks to security, to privacy, and to trade secrets may need to be considered.

Internet of Things

Obtaining a legal ground in compliance with GDPR/eprivacy for such systems might again be difficult in scenarios in which personal data is processed for one or more specific purposes – such as in high-frequency communications between multiple actors in machine-to-machine (M2M) or vehicle-to-everything (V2X) communications. Upholding a valid consent may prove to be impossible with interconnected systems, as persons in those systems are not always active users that can accept consent forms. The GDPR principles of storage and purpose limitation and especially data minimisation are also difficult to implement. On the contrary, the Internet of Things is based on 'data maximalism', meaning the collection of vast amounts of personal data, the creation of unique user profiles and the scanning of devices.

Blockchain

One key property of Blockchain technology is that old data can be secured against modification, making it an append-only structure where new data can be added but never removed. Thus, blockchain runs counter to the GDPR's 'right to be forgotten'. Once personal data is recorded in a decentralised block, it is no longer possible to delete that information. This historical data can then be analysed to reveal identities. While the GDPR enforces its rules against at least on specific person, blockchains involve numerous actors, which makes the allocation of responsibility/accountability very hard, if not impossible. The concepts of the GDPR (controller, joint controller, and processor) can hardly map this. Because blockchains are constantly growing, the principles of data minimisation and of purpose limitation can also not be fulfilled. Lastly, it is often unclear if data that is stored on a distributed ledger or that is encrypted or hashed still qualifies as personal data.

Biometric data

Applications based on, facial or voice recognition or personal data generated by wearable devices regularly do not fulfil the existing data protection rules. In many areas, the risks linked to biometric data even lead to a general prohibition of any form of processing. The GDPR also does not distinguish between one-to-one biometric comparisons (e.g. verification) and one-to-many comparisons (e.g. identification). The legal/technical definitions are also diverging and there is uncertainty over which type of data qualifies as 'sensitive'. If this field is regulated by a new AI framework, legislative overlap needs be avoided.

Virtual reality

This combines the problems already listed on the processing of biometric data with the

question whether consent is really freely given, meaning that it is unclear if the data subject had a real choice to refuse the processing of personal data.

Text and data mining

The use of text and data mining is not compliant with the GDPR because one cannot be sure that the method is not also processing personal data. The controller will have difficulties to fulfil the transparency obligations as text and data mining leads by definition to the processing of unknown data. Notifying the affected data subjects and getting an informed consent will be very difficult. It is also important to distinguish between text and data mining for scientific reasons and for commercial use as both approaches have different effects on data protection and should have different transparency requirements.

Profiling and micro targeting

There is a lack of distinction between automated processing, including profiling, which is expected by individuals and which contributes to more effective services to individuals and more relevant content, and profiling which creates harm, such as political manipulation, or a commercial lock up effect for which specific safeguards should be put in place. In case the latter is being addressed by new legislation such as the Digital Services Act, legislative overlap with existing GDPR / ePrivacy provisions should be avoided.

Cloud computing

The GDPR links the processing of data either to a single person in charge (Art 4 Nr 7 GDPR) or determines special provisions for situations with multiple persons (Art 26 or 28 GDPR). Both approaches are not sufficient for cloud computing. This problem is aggravated by the fact that multiple parties are involved without clearly assigned qualifications and that data is constantly moving within interconnected clouds while temporarily stored on different physical locations in different countries. The problems specified in Chapter X of this paper complicate the use of this technology further.

Home-office

Employees often do not have genuine data protection expertise and are thus left alone with conflicting responsibilities and many new obligations in a situation in which private as well as business data is being merged. As a result, they are often violating GDPR provisions unintentionally. Many employers do not step in as they want to save costs or do not want to overburden their staff with new rules, procedures and obligations.

III. SMEs & start-ups vs digital gatekeepers

In combination with the ePrivacy Directive and settled case law, the GDPR led to a proliferation of cookie banners and many different types of user consent interfaces, while the other five legal grounds for processing data are not frequently used. As a result, the already existing **vendor lock-in** in the digital economy was further consolidated. This consent-based approach has created high regulatory burden for SMEs and start-ups, as well as placing them at a substantial competitive disadvantage against large consumer-facing corporations. These digital gatekeepers are in a position to offer multiple integrated online services, providing a better and smoother experience for users who are in return more likely to give them their consent when wanting to use one of their services.

Digital gatekeepers have many external consultants as well as large legal departments with data protection experts. **SMEs and start-ups** by contrast often **lack** the **knowledge, capabilities** and **financial resources** to implement GDPR rules adequately or to go to court over potentially non-compliant services. Consequently, they face a much greater risk of sanctions than their big competitors do, while the fines at the same time pose an existential risk to their businesses. Another side effect which puts SMEs and start-ups at a disadvantage is that they might choose to direct resources to hire external legal experts to ensure compliance with the law, rather than investing those resources into recruiting data scientists to innovate / improve their products and services.

The high compliance costs as well as the legal uncertainty effectively **hinder innovation** for SMEs and start-ups. Studies have proven that the GDPR has strongly affected business models and investor confidence, resulting in entrepreneurial discouragement and the abandonment of products.[1]

[1] In the Google Play Store, about 1/3 of all available apps needed to be taken off. The entry of new apps fell by 50%. Read more under http://conference.nber.org/conf_papers/f146409.pdf. See also how the GDPR effected start-up innovation under https://link.springer.com/article/10.1007/s10796-019-09974-2.
GDPR made the market for web-tracking more concentrated, with Google gaining the most market share among large providers: https://voxeu.org/article/how-gdpr-affects-global-markets-data
GDPR increased ad vendor market concentration by almost 20% https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-garrett_johnson.pdf
GDPR caused a 40% drop in the average amount of VC funding and a 20% drop in the number of VC deals in Europe for newer, data-related, and business-to-consumer ventures. https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment

The exemption of keeping records in Art 30(5) GDPR for SMEs with fewer than 250 employees is practically ineffective, as each company with an IT infrastructure will not only occasionally process personal data. 'Not occasionally' is understood very broadly, meaning that it already includes emails, payroll, customer management or event logging of the operating system. Moreover, every company with employees regularly needs to process special categories of personal data such as health data in the context of continued pay or information on religious affiliation as part of payroll tax. Since the exemption rule is not applicable in those cases, the intended relief for SMEs does not materialize in practice. For the numerous other obligations besides Art 30(5), there are no SME exemptions at all. The lack of a materiality threshold that differentiates between the various types of risks and the scope of the processing of personal data as well as the type of the company is also difficult to comprehend.

The issued guidelines by the EDPB and DPAs on the exemption in Art 30(5) GDPR and on other issues are not always helpful for SMEs. An elaboration of appropriate analysis frameworks of each type of technology forces SMEs and start-ups to execute their own impact studies after reading more than 60 pages of guidelines, which is neither feasible nor pragmatic. Simplified and more structured frameworks are missing.

The lack of interoperability mechanisms and effective implementation of the data portability rights is preventing SMEs and start-ups from breaking up data silos in order to increase their own competitiveness. The economy-wide data portability rules of the GDPR require personal data across all sectors to be in a "structured, commonly used and machine-readable format". This creates a regulatory burden, as sector-specific rules would be much more adequate for data exchange. At the same time, also the envisioned scope for data portability might not be feasible in practice. Originally meant to help to switch between social networks, it has been extended beyond this specific area of application without helping to empower individuals. The concept of data portability will only work when there is an obligation for both export and import of personal data. Even the transfer of personal data outside of the EU within a company network is complicated, as it demands the same contractual requirements as an external data transfer to another entity.

The GDPR lacks a mechanism that allows SMEs and start-ups to shift the compliance burden onto third parties which then store and process data. IT solution providers

could take on the responsibility from SMEs and start-ups, thereby allowing them to assume compliance just by paying for and using their services. Currently, the use of such services results in a complex inter-relationship of liability, meaning that SMEs and start-ups would often still have to bear the burden of compliance.

IV. Private citizens and voluntary entities

Numerous new obligations and the need to invest significant time and money to guarantee GDPR-compliance means high regulatory burden for societies, clubs, associations and private citizens. Those demands regularly bear no proportion as those entities and persons are not processing personal data commercially and are often spending their spare time as volunteers for a good cause.

Despite their lack of adequate resources and knowledge as well as the reduced risk level, those actors are still required to execute numerous tests such as fairness assessments, the weighing of interests, compatibility verifications, necessity reviews, appropriateness tests or risk reviews. This shows again that some legal requirements established by the GDPR have completely lost sight of the practical realities.

Since Art 13 and 14 GDPR are generally applicable, the websites of private citizens and voluntary entities require extensive information disclosure, which increases the length of privacy policies but not necessarily the readability and intelligibility of privacy terms for individuals.

To get professional help, voluntary entities and private citizens are often hiring data protection consultants or specialised law firms in return for high charges. Instead of offering free-of-charge Privacy Policy templates that guarantee GDPR-compliance, the EU thus created a new business model that is based on an obligation-overload for ordinary citizens and voluntary entities. The published guidance by DPAs is also not really helpful, as the addressed actors lack time and expertise to fully understand and implement those complex documents.

The household exemption (processing personal data "by a natural person in the course of a purely personal or household activity") is too narrowly defined, since according to the case law of the ECJ, publication on the internet cannot constitute a purely personal/family activity. The more relevant question of whether the personal data is processed for non-commercial purposes only is not taken into account.

Since every exchange of information contains the personal data of both the sender and the recipient, the GDPR (together with the ePrivacy Directive)

affects communication on the internet per se. Thereby, data protection often even prevails over the freedom of expression. Exceptions in the form of opening clauses regarding the freedoms of communication (Article 85(2) GDPR) were only used by Member States for the traditional press but not for the processing of private data by bloggers, amateur photographers, public relations and other private users.

V. The guardians: EDPB & DPAs

Data protection authorities are too one-sided and too much focused on the protection of personal data. Although this is of course their main purpose, they should be obliged to also take other elements such as fairness, equality, health, security, competition, prosperity and innovation into consideration.

On the one hand, the **'one-stop-shop'** principle proved to be key in providing legal certainty and reducing the administrative burden for companies and citizens alike. On the other hand, it helped big companies to escape liability due to the reluctance and/or the disproportionate workload of certain DPAs to undertake investigations and to impose sanctions in fear of losing investments in their countries. As reasoned by the CJEU Advocate General, other concerned DPAs should also be allowed to play an active role in scrutinising organisations' compliance with the GDPR and thus, supporting the leading DPA of the country where the company is based. It is important to underline that the described problem is not related to flaws in the law but to a lack of consistent application. The cooperation and consistency mechanism - laid out in Chapter VII of the GDPR - offers procedures that would help to prevent forum shopping and to involve DPAs from other countries. However, the EDPB and the DPAs are rarely using this important tool so far.

Another reason for the inconsistent and weak GDPR enforcement - in some Member States only 0.15% of the complaints about data breaches are investigated - is the fact that many national **DPAs are underfunded and understaffed**.[2] They are often unable to deal with the massive increase of tasks and, in particular, to enforce, prosecute and punish data protection violations in a meaningful way. To guarantee a European level playing field and to safeguard companies from existence-threatening waiting-times, every DPA should have a sufficient and adequate level of human, technical and financial resources, premises and infrastructure. They should also concentrate their resources on major cases.

If an **investigation** takes place, the legal opportunities and dimensions of penalties

[2] In February 2020, the EDPB published the contributions of EU DPAs to a questionnaire evaluating GDPR, in which 14 DPAs declared that they were not being properly equipped to contribute to cooperation and consistency mechanisms. See also: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

are however not reasonable and questionable in rule of law terms. The powers of intervention of DPAs are in fact unprecedented if compared to other regulatory offences. They even exceed the highest possible fines under criminal law. Moreover, the DPAs have access to all information and personal data as well as to all the controller's premises and data processing equipment, allowing them to effectively shut down businesses by banning their data processing or by imposing lengthy investigation and compliance procedures, which can place a company at a disadvantage on the market. All these powers are hardly limited or specified by law while a lot is being decided based on administrative discretion. Furthermore, the directorship of a DPA is a political position, filled with person with political background. However, this person is often without any experience in data protection, as there is no requirement for specific knowledge like in many other public positions. Against this background, it is even more surprising that DPAs are not subject to neither technical nor legal supervision, as is usually the case with regulatory authorities. Instead, they enjoy complete independence. Similar assessments can be made about the EDPB, as its opinions have substantial impact on European data processing without having democratic accountability and legitimacy. While the EDPB's opinions are non-binding, they have the purpose of steering a harmonized interpretation of the GDPR across the EU, and are often directly referred to in DPA guidelines, thus de facto becoming legislation enforced by DPAs. Therefore, it is highly concerning that there is currently no recourse possible against an EDPB opinion due to its non-binding nature.

Driven by political opinions and motives of some employees, the EDPB and several DPAs were publishing some very strict interpretations of the GDPR, which were clearly against the will of the legislator and in violation of the principle of neutrality. Noticeable is the fact that, while the EDPB in theory should consult all stakeholders for the development of its opinion, in practice, it has been very unresponsive to stakeholders from research, industry or civil society and their calls for balanced interpretation, rarely considering their feedback, or running a consultation after having already adopted the opinion. To balance out the EDPB, which has shown itself to be one-sided, a European Data Innovation Board should be established. It should feature representatives from research and industry, and have a statutory remit to issue comments, interpretations and guidelines on how to balance the fundamental right to privacy against the rights to life, liberty, security, and the freedom to conduct business in Europe.

There is also the tendency from certain DPAs to publish guidance and consultations separately on similar topics (e.g. on cookies), which does not create an environment conducive to innovation. Until courts are able to dismiss those interpretations, companies already adapted or even stopped the criticised processing of personal data. In practice, DPAs often also do not comply with the law that regulates under which conditions public bodies are allowed to express themselves. There are many cases, in which companies that have been fined, were denounced by name. Some companies have even been publically warned without having been proven to have committed a violation against data protection rules.

Especially when it comes to SMEs and start-ups or when a breach occurred for the first time, DPAs should work more service-orientated with warnings, explanations and offering help on how to become GDPR compliant. Similarly, not every incident is a data breach. Due to the fear of being sanctioned, companies tend to strictly interpret notification rules and are 'over-reporting' (thereby further straining DPAs' resources). It is further problematic that fines by DPAs for data breaches are more and more accompanied by civil law claims for damage, especially in form of collective redress claims. Not every small data breach should be a target for a claim for damage, in particular if those lawsuits are run by commercial actors that hope to make profit on the back of the affected data subjects. The scope of Art 82 GDPR has proven to be too vague.

The roles and obligations of DPAs, their lack of resources to guide companies, and the complex procedures complicate cooperation between DPAs and the industry. Firstly, the dual role of DPAs as both an enforcer and advisor to industry means that they are vested with investigative and corrective powers to enforce the GDPR, while also having an advisory role. Audits or evaluations meant to provide guidance and support may instead lead to the identification of non-compliance cases, followed by enforcement measures, likely resulting in the imposition of fines. This may challenge trust in the relationship between DPAs and companies. Secondly, under-resourced DPAs may not be able to provide efficient guidance, as they might prioritize focusing resources on handling complaints rather than on engaging constructively with companies. As a result, companies that do not receive responses swiftly may experience delays in moving through development cycles.

VI. Fragmentation

To start with, like with many other legislations, the European Union faces challenges due to language barriers, cultural differences, outdated information exchange systems, divergent national legal systems and diverging methodologies such as for data protection impact assessments across Member States.

When further specifying the application of the GDPR in certain areas (e.g. the age of consent of children for online services), many Member States have introduced legal requirements on top of the GDPR rules in their national sectoral laws. This stands in the way of a genuine harmonisation of data protection rules. It also leads to even more legal uncertainty, especially for companies that offer products and services in various Member States.

Besides the different interpretations of the law, the enforcement and the level of fines issued also vary significantly between Member States. This situation enables companies to settle in those countries that have the 'sloppiest' GDPR implementation combined with the lowest fines.

The penalties based on GDPR violations are often not adequate. While the fines imposed on some multinational companies are sometimes too low to serve as an effective deterrent, already the threat of a fine can be existential to a SME and force it to give up its business idea. What is missing are clear criteria to define when a violation took place and on how to set the exact amount of the fine.

Many GDPR provisions (e.g. Art. 15, 20, 24, 25, 26, 32 GDPR) do not meet the requirement of sufficient clarity and definiteness, allowing various contradicting interpretations that cause legal uncertainty. This is a considerable disadvantage not only for the user of the law, but also for supervisory authorities. In other cases, concepts were not harmonised enough. Below some of the most urgent examples:

- There are very different interpretations by national DPAs on what constitutes a valid 'consent', whereas some of those greatly diverge from European legal traditions and civil law principles.
- Some DPAs apply very restrictive interpretations of 'legitimate interest' that for instance rule out data processing for purely commercial interests (although Recital 47 GDPR lists direct

marketing as an example of a valid use of 'legitimate interest'[3]), or that hamper video surveillance of retailers to protect costumers against pickpocketing.

- The DPA guidance on cookies and on data protection impact assessments is also not consistent, leading to a situation in which companies have different documentation obligations among Member States.
- Fragmentation can also be observed in the lack of technical standardisation of the rights of the data subject (e.g. through the provisions of APIs based on Art. 21 (5) GDPR), on privacy policies obligations for websites or on formalities for data breach notification forms.

[3] In this case, the interpretation of the Dutch DPA was later overruled and invalidated by a Dutch court. In his judgment, the court explained that having a commercial interest, does not automatically exclude legitimate interest as a lawful processing ground.

VII. Flaws and gaps in the legal text

Anonymization

Although the depersonalisation of personal data in large numbers could be a crucial means to guarantee both data protection and a thriving data economy, the GDPR does not offer much guidance on this. Recital 26 just states that the law is not applicable to anonymized data.[4] Further legislative clarification is needed:

- Standardized definitions of absolute and relative anonymization and a further differentiation to pseudonymization is needed. It should also be clarified that the law only demands a relative anonymization for a GDPR-compliant depersonalisation process as it is already stated in Recital 26.
- The definition of 'personal data' under Art 4(1) GDPR remains extremely broad while being unclear on the conditions for datasets containing personal data to be considered as anonymous.
- Some decision makers and data protection authorities consider the process of rendering personal data anonymous also as 'processing' in terms of Art 4(2) GDPR.[5] This would mean that depersonalisation would also require a legal basis, which would needlessly complicate the whole process.
- Anonymization is, moreover, a purpose-changing further processing. This means that, according to Art 6(4) GDPR, the processing must be compatible with the original purpose, based on the original legal basis.
- In addition to these four legislative issues, the EDPB should also release practical guidelines on which specific standardized anonymization methods can be used to render data anonymous according to the GDPR. The WP 216 of the Article 29 Working Party proved to be insufficient in practice. Specific use cases and relevant situations for different types of data processors and a checklist with all requirements that have to be fulfilled to make data anonymous should be included.

[4] In particular, the lack of specification in the law as well as guidance on the following part in Recital 26 does lead to legal uncertainty in practice: "*to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used*."
[5] The German Federal Data Protection Commissioner, for instance, stated this understanding of Recital 26 in his latest position paper on Anonymization in the GDPR, dated from 26 June 2020.

Regular updates seem to be necessary as the technical developments in this area are speedy.

Mixed data

Due to the huge legal uncertainty as to whether personal data is sufficiently depersonalized, companies are often deciding not to share any of their commercial datasets as they contain mixed data. The GDPR determines that its provisions apply when personal and non-personal data are 'inextricably linked'. Despite new guidance, it is in practice however very difficult to clearly distinguish between personal and non-personal data or to extract both from each other.

Secondary use

Especially in times of COVID-19 and the use of data in health care but also for areas such as cybersecurity or Artificial Intelligence, Recital 50 and Art 6(4) GDPR proved to be highly problematic. In practice, it is often unclear whether a new legal basis is required for cases in which the data subject has initially given consent but where the personal data is further processed for another compatible purpose than the purpose of the initial collection. The narrow interpretation of consent as well as the vague criteria for the compatibility assessment (conducted by the controller/processor) result in numerous situations in which extremely useful data for the good of society cannot be used. Even worse, many DPAs even ignored the fact that compatible further processing is allowed under the GDPR provisions.

Rights of the data subject

Several provisions in Chapter 3 did not lead to an improved legal situation for the data subject but instead overburdened the controller. Therefore, legislative changes seem to be useful:

- The requirement of information disclosure in Art 13 and 14 should not apply when the purpose of processing of personal data is obvious from the context of collection (e.g. distributing business cards on a fair or initial telephone call with clients), if the data subject already has the relevant information or if the interest of receiving information can be regarded as low according to the circumstances.
- The current requirements in both Articles also lead to very complex and mostly confusing data protection declarations on websites that do not help data subjects in terms of transparency or trust. Studies show that the willingness to

read privacy statements is declining since the GDPR is applied.[6]

- It is also not comprehensible why - especially in low-risk processing scenarios or when SMEs, start-ups, non-commercial entities or private citizens are the controller - there are no exemptions (such as those in Art 14(5) GDPR) in Art 13. Especially, information and advice centres (e.g. addiction, sexual violence) and their clients are suffering under the lack of sufficient exceptions.
- There is a general lack of provisions that protect the rights of the controller and of third persons (such as business and trade secrets or confidentiality obligations). Exemptions, to avoid disproportionate efforts, are therefore also missing in Art 15 - 18. In practice, especially the large scope of Art 15 (right to access) is leading to problems as even mere backup copies, personal data that the data subject can access at any time (e.g. account transactions, contract details) or personal data that is not directly stored in the system (e.g. name of the data subject was mentioned in an email) are covered by that article.

Controller and processor

In practice, the unclear distinction in Chapter 4 of the GDPR between controller, joint controller and processor causes many problems:

- The definitions in Art 4 No 7 and 8 GDPR are too vague and guidelines including case groups are missing.
- In cases of joint controllership, the market power of the controllers, their ability to influence processing and arrangements on a practical level are hardly taken into account, while the legal obligations and conditions for such a cooperation remain unclear. In particular, market power has allowed large tech companies to impose joint controllership, with commercial terms, to smaller actors on the market.
- In complex projects involving several cooperating companies, the differentiation between joint-controllership and processing is often blurred. Harmonised guidelines are missing here. The contractual requirements for processing in Art 28(3) GDPR are moreover not distinguishing between the specific risks of different types of processing. Exemptions for low-risk processing

[6] See Eurobarometer from May 2019: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86881

(such as IT maintenance) are also not provided by the GDPR. The processor's duties to record in Art 30(2) GDPR seems superfluous as the required information is already in the processing contract.

- The requirements laid out by Art 25 GDPR remain unclear and fail to reflect the reality of software development and digital services. Although software or services are often designed or offered by non-European companies (such as 'Google Analytics' by Google), they are hardly covered by the GDPR. This means that those actors are often able to shift their liability on European companies that are deploying the software or utilize the services, without having any control on the data protection by design and by default. Moreover, Recital 78 only mentions data minimization and pseudonymization as adequate means. However, the field of 'privacy enhancing technologies' has created many alternatives, from synthetic/augmented data to anonymization and federated learning.

Breach notifications (Art 33–34)

The provisions on data breaches leave many questions unanswered. The relationship between the obligation to report data breaches and the freedom of self-incrimination as well as the use of information for subsequent investigations remain unclear. The articles are further lacking clear material thresholds (e.g. professional secrecy, suspected criminal offences, credit card accounts or passwords) in order to confirm a notifiable personal data breach; they do not follow a risk-based approach by requiring immediate reporting even for minor breaches; and they are not offering any mitigating circumstances as incentives for companies to report data breaches. Furthermore, the data breach notification forms, the way of how to inform the data objects and how to provide remediation are highly fragmented, leading to unfair results and making cross-border cases very difficult to solve. Lastly, the 72-hour deadline for breach notifications is highly impractical and binds resources that a company could use to analyse and remedy the harm. Before fulfilling the obligation to notify the authorities, the company should make it a priority to fix the data breach.

VIII. Data protection in the health sector

Medical diagnoses and treatments are highly dependent on genetic and medical factors. For instance, women may react differently to medication than men do. The existence of pre-existing conditions, certain genetics or medical factors have a huge influence, if not on a diagnosis at least on the reaction to a treatment. Therefore, especially the health sector depends on large amounts of personal data. A drug or a vaccine has to be tested on people with for instance pre-existing conditions just as much as on those without, in order to check its safety for everyone. Since most health data is pseudonymised, many additional legal steps, checks as well as time and purpose limitations were introduced by the GDPR. The effects are obvious: the entire health sector suffers from legal uncertainty and is heavily restricted in its crucial work. The most reasonable solutions would be create a specific new chapter on health in the GDPR or to exclude medical research as well as medical and healthcare professionals completely from the GDPR and to come up with a sector-specific law on data protection for this specific area. Addressing all problems - some of them are listed below - while keeping the GDPR applicable seems to be a rather impossible endeavour.

While Art 9(1) GDPR forbids the processing of special categories of data, including health data, the exception clauses in paragraph (2h) and (2i) are very vague and leave the exact elaboration in the hands of the Member States. The result is legal fragmentation across the EU. Researchers and hospitals often do not know which rules apply in a Member State, in particular if it has a federal system.

The processing of health data - based on a contractual relationship - creates many new problems for practitioners, as Art 9(2) GDPR requires them to get additional consent by the affected person in most cases. New research projects are thus regularly delayed, as additional contractual arrangements need to be negotiated first. As researchers cannot do it themselves, they need to hire (often expensive) lawyers in order to place the necessary safeguards.

The legal situation for a scientific discovery (involving personal data) that can have an effect on another disease, drug or treatment is uncertain. The original consent was not given for that purpose and thus, cannot be used as the legal basis again. Do researchers need to request the approval of all providers of personal data again due to

their unforeseen use or can they use public or legitimate interest as a legal ground? What happens with data that was collected prior to the GDPR; in particular, when the researchers are not able to go back and track the affected patients?

Medical research projects involve the sponsor of the trial (e.g. company), who is responsible for supervising and managing it. However, also other involved parties (collaborators) as well as external hospitals are handling the clinical trials on the ground. In practice, it often remains unclear which actor in this network is responsible for the data sharing agreements and in which of the numerous parallel contractual agreements between those actors it should be placed.

Data from patients with a chronic disease that have a medical device is not automatically pseudonymised. However, more and more hospitals are asking their patients to pseudonymise the data in order to rule out any GDPR breaches. Yet many patients would be willing to provide their personal data without any depersonalisation if this is beneficial to them or to the patients' community. On the other hand, it is not always clear to the patient what data provision agreement the medical device is used on and if the personal data is shared commercially and/or with third countries. This point is particularly relevant when non-European cloud providers are being used, which again cooperate with additional third party suppliers.

Finally, it is also legally unclear whether profit-seeking companies that are carrying out important scientific research fall under the category of 'scientific research' as defined in Recital 159 GDPR.

IX. Practical Problems

Certificates

Although the GDPR offers the framework for companies to prove their GDPR compliance (Art 42/43), there is still no generally accepted certificate. Codes of conduct as an alternative option are also not commonly used due to their lengthy and costly adoption procedure, as well as the highly uncertain outcome of such an effort. While companies can barely use their high data protection standards as a competitive advantage, customers are forced to do extensive reviews on their own and are frequently falling for frauds. A trustworthy certification, based on international certification standards (ISO 17024), should also cover the qualification of the DPO.

Training and role of DPOs

A standardised basic training concluding with a centralised exam is missing. There are also limited requirements for becoming a data protection officer in a company as well as too vague clarifications in Art 39 GDPR on the exact tasks and responsibilities of the DPO. In practice, the DPO can often not fulfil the role of checking and maintaining the records of processing activities as the necessary substantive statements are not provided.

Data protection impact assessments

According to the GDPR, it is the company itself, which is performing the DPIA, while the DPO is just assessing the result. The leadership of a company is often not aware of the benefits of giving the DPO a more supportive role in the whole process. DPOs could, for instance, help to assess the risks for data subjects and give guidance on how to create protective measures.

Advertisement

The processing of personal data within online advertising has to rely almost exclusively on consent, ignoring the other legal bases in the GDPR. This approach ignores all distinctions between first and third parties processing data, and their relation with users (or lack thereof). In addition, large tech players, who can obtain consent more easily, or though forced joint controllership with smaller but consumer facing partners, can often carry on processing the data under a different legal basis for their own competitive advantage.

Data portability in the finance sector

The right of users to request that their provided and stored data is being transferred directly from one data holder to another in real-time, as granted by the PSD2, is not fully functioning in practice yet. What is missing are sufficient technical interfaces that allow the portability of data in real-time.

Deletion of data

The requirement to 'delete' data is sometimes impossible from a practical perspective. Together with the limited guidance that is provided on what may be "reasonable" in Recital 66 and Art 17 GDPR, it places a large administrative and operational burden on companies, which are either unable to delete personal data because it would 'break' their systems or which have to build disproportionately expensive new systems to enable some kind of anonymization.

Unfair competitive advantage

Certain companies that are active in the European Single Market are exploiting the fact that some third countries do not have a high level of data protection. They are building research centres in those countries to train their AI or to test their new data-driven business models without any restrictions. By doing so, they are able to strongly advance in technical terms and eventually introduce these technologies in the EU in order to capture significant market shares in the Single Market.

Abusing the right to be informed

Some professional providers pursue their commercial self-interest by incentivising data subjects to exercise their right to be informed against undesirable competitors. This form of vigilante justice is possible due to the missing formal requirements for exercising this right (e.g. via social media platforms) as well as the indefinite scope (e.g. unclear whether handwritten notes are included).

X. International data flows

In order to show their GDPR compliance, many companies state that personal data will not be transferred outside the EU, although their data traffic passes through third countries or is saved in global cloud services. Understanding and monitoring such processes is highly complicated and expensive, especially for SMEs. This is aggravated by the fact that data protection authorities argue that the risk-based approach does not apply to international personal data flows (Chapter 5) as well as by the recent Schrems II ruling by the ECJ. In practice, this contentious interpretation means that most transfers of personal data to third countries require companies to execute a comprehensive risk analysis and appropriateness test.[7]

Adequacy decisions would be an excellent means to simplify international data flows since they do not attach data transfers to additional conditions or authorisations. Nonetheless, the European Union has only concluded them with twelve countries so far, although many additional third countries have recently adopted new data protection laws with similar rules and principles as the GDPR. This is also due to the lengthy and complex process of adequacy assessments and following negotiations, which might discourage countries from wanting to become a candidate altogether. Another problem is the inconsistency when it comes to the assessments or the reviews. While the EU did not react after it became aware of non-GDPR-compliant data processing in some countries, others with similar or even less problematic actions were pilloried in public by DPAs and politicians.

Transatlantic data transfers are crucial for many businesses as well as for digital services and applications that people are using on a daily basis. In light of a lack of competitive alternatives from within the EU to dominant services from third countries (e.g. Google Ads, YouTube Video Hosting), the Schrems II judgement of the ECJ has brought great uncertainty over such transfers and put many European SMEs, start-ups, universities and research institutes, which had relied on this particular adequacy decision, in a legal limbo. European multinational companies also suffer from increased uncertainty around

[7] Which are however not necessary if an adequacy decisions exists or a derogation based on Art 49 GDPR applies.

transfers with their US subsidiaries and business partners.

In the absence of adequacy decisions, standard contractual clauses (SCC) are the most widely used tool for international data transfers. The EDPB recommendations on supplementary measures, however, disregard the GDPR's risk-based approach to security measures (Art 25(1) and 32(1) GDPR) and require encryption and full unreadability of personal data at every stage of processing data outside of the EU. In combination with the Schrems II decision by the ECJ, companies are now obliged to undertake 'mini-adequacy' findings for each of their data transfers (as they are required to assess the laws of the country of destination themselves and on that basis, decide which safeguards would be the most appropriate). This is simply not feasible in practice.

Codes of Conduct, Binding Corporate Rules (BCRs) and certification mechanisms[8] are hardly used as potential alternatives to adequacy decisions. In cases of codes of conducts and certificates, missing guidance and political motives can be named as main reasons. The EDPB has so far not even approved one. For BCRs, the bar for the creation and implementation - as is determined by the DPAs' Working Papers - is too strict, complex and narrow for the realities of a digital economy.

The understanding of the derogations in Art 49 GDPR is another case, where the EDPB's interpretation goes beyond the will of the legislator. For instance, Art 49(1a) permits data transfers on the basis of the data subject's explicit consent after having been informed of the possible risks of such transfers to third countries wherein the level of data protection is not adequate. The exceptional nature of this provision is already accounted for through the increased informational requirements compared to consent pursuant to Art 6 and 9 GDPR. Although there are no restrictions on the possibility of consent neither in the wording of Art 49(1a) nor in the related Recitals, the EDPB guidelines only allow consent in exceptional cases.

[8] Sufficient for international transfers if complemented by binding and enforceable commitments of the controller or processor in the third country that guarantee that they will apply the appropriate safeguards.