Wilfried Martens Centre for European Studies

May 2018

IN BRIEF

The Impact of GDPR on Users and Business: The Good, The Bad and the Uncertain

Dimitar Lilkov

It's official. The General Data Protection Regulation (GDPR) has started to apply directly in all member states with the aim of safeguarding the processing of personal data of all natural persons within the European Union. The Regulation is seen as the most comprehensive 'upgrade' of data protection rules over the last two decades as it repeals Directive 95/46/EC enacted in the distant 1995. GDPR standardises and strengthens citizens' rights when it comes to collecting and processing personal data while also empowering national data protection authorities to supervise this new ambitious framework, by enhancing their responsibilities and ensuring the possibility of heavy fines at their disposal. European and global businesses (big and small) had two years to adapt to the new onerous requirements which demanded administrative, technical and even strategic changes in the way they operate. The following In Brief aims to highlight the essence of the Regulation's 99 Articles and analyse the potential impact of GDPR on both users and business.

An opportunity for users

The main feat of GDPR is its subtle aim to announce that in the modern digital economy personal data is essentially a resource which should be regulated systematically especially when it comes to processing, storage, deletion or transfer to third countries. Even though a bit late with this legislative endeavour, the EU is catching-up with the reality of today and attempts to roll-out the most ambitious personal data regulation globally.

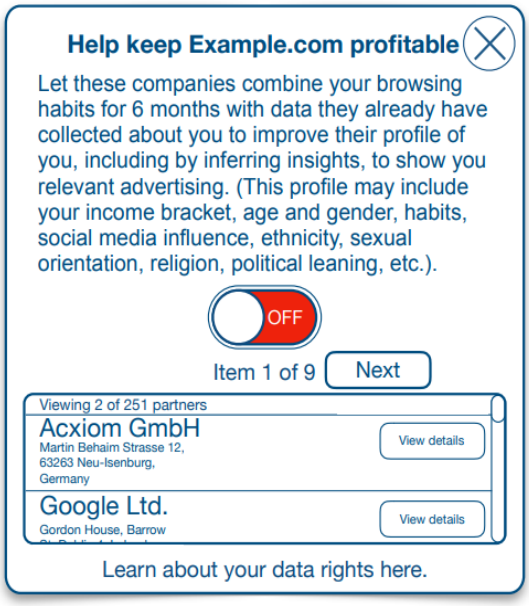
From a user's perspective, GDPR should be lauded as a leap forward. The new legal obligation for data protection 'by design and by default' compels public bodies, organisations and companies to change the way they approach the processing of personal data and consider privacy at the earliest stage possible. A service should only require the minimum personal data required for the performance of said service and not request information which goes beyond the necessary. This is a complete rethink of the current architecture of websites and services which often encourage the disclosure of too much personal data. There is an inherent incentive for

companies to accumulate maximum volume of specific personal data (age, race, religion, political views, device location, etc.) which can be cashed in a later stage via targeted advertising or through selling bundles of data to third parties. Traditionally most online services have been collecting and sharing data with little actual restrictions as regulators did not have the necessary mechanisms to enforce privacy rights.

As companies have been preparing for the new rules to kick in we are about to see a number of improvements when it comes to enhanced user tools and privacy controls. The Regulation gives additional possibilities for users to manage their data and request information on what type of data is stored and how it is eventually used. With the option to download all the data a company has on you, a user can double check what is being stored and make use of the possibility to export his/her data to other services. There is also a range of additional reinforced user rights[1] and to analyse them in detail goes beyond the aims of this current In Brief. However, special emphasis should be placed on the importance of the user's valid consent which is at the heart of GDPR and remains crucial when it comes to ensuring digital privacy in the long run.

The provision of valid consent by the user is a fundamental condition for the further processing of personal data but also remains one of the most elusive concepts laid out in the Regulation. The provided consent should be informed, unambiguous, specific for every purpose and given by a clear act. This specific permission must be requested in an obvious manner and not be bundled together with other purposes – in case the processing of personal data has multiple purposes, valid consent should be given separately for all of them. This is a clear departure from today's reality in which a number of services ask for your general consent to their terms and conditions, for example, and use this as a legal proof that you have accepted all of the personal data provisions as a bundle. In reality very few people read the enclosed documents and have no idea to what they are actually giving permission. GDPR provides for specific separation of these purposes in order for the user to be able to have the choice to opt-in or opt-out to some of them. The official working group which issues guidance for GDPR interpretation advises that 'the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of purposes and obtaining consent for each. [2]

Figure 1 Potential design of a consent form based on granularity and providing informed choice



Source: J. Ryan, 'GDPR consent design: how granular must adtech opt-ins be?', PageFair, 08 January 2018, last accessed on 16 May 2018 at: https://pagefair.com/blog/2018/granular-gdpr-consent

[1] Such as the right to transparent information, the right to erasure, the right to object to automated decision-making or protection of personal data sent to third countries.

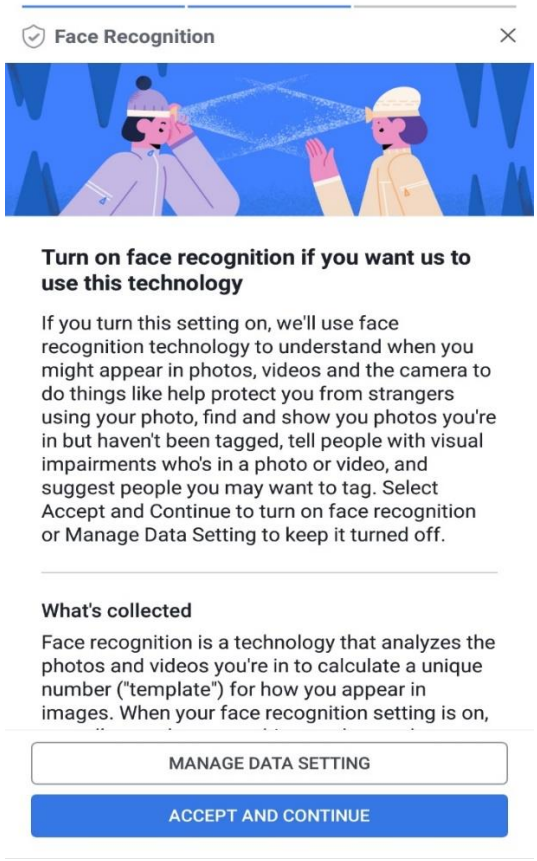
[2] Article 29 Working Party, '*Guidelines on consent under Regulation 2016/679*', European Commission, November 2017, p. 11. Last accessed on 16 May 2018 at: https://goo.gl/qLpuyR

Figure 1 provides for a good example of appropriate design. Silent approval of the users, denying them a clear choice or enforcing their consent by default should all be considered as a breach and the given consent rendered as void.

The open question is about the actual implementation of these new requirements. What would be the threshold for recognising consent as valid and free by the national regulators?

How are regulators and courts going to interpret the strict provisions for free and valid consent by the user? The ball is now clearly in the court of national data protection authorities which will have to face complex decisions. The additional example below illustrates this point (Fig. 2). The image shows how a social media company has recently (prior to the entry in to force of GDPR) requested user consent for one of its services. As seen, there is no direct option for declining this additional feature straight away as the design is nudging the user to 'accept and continue'. Only by going through the additional data setting can you find the option to opt-out of a feature which otherwise would be allowed to scan your facial features and automatically recognise you in pictures. It can be argued that the choice is pre-defined and is misleading for the user. Would the consent given constitute as free, clear and informed under GDPR which is now in force?

Figure 2 Request for user consent asked prior 25 May 2018. Will this be valid consent under GDPR?



Source: Screenshot from personal Facebook account, Face recognition consent prompt, Facebook

A potential curse for business?

What about businesses? GDPR could be seen as a positive development for companies and services, as well. Compliance with the new provisions can be a chance for improved data management and spark new business models. A global study [3] of executives across a number of industries highlights that managers perceive the new legislation as an opportunity for gaining customer trust and GDPR compliance could serve as a positive differentiator in a competitive environment. Companies would most likely

[3] IBM Institute for Business Value, '*The end of the beginning: Unleashing the transformative power of GDPR'*, May 2018, p.2. Last accessed on 16 May 2018 at: https://goo.gl/QPxDWz

cut down the amount of personal data they keep and would need to revamp and improve their internal processes which should be beneficial for both business and consumer in the long run.

However, GDPR compliance will certainly demand heavy financial and technical investment. Sending out e-mails to your customers for re-validating their consent is just the tip of the iceberg. Every company or service, regardless how big or small, will have to invest in software, technical support and legal advice to ensure compliance. The new provisions for processing personal data and strict timelines for businesses to identify and report security breaches to authorities would be especially costly for the big companies. Preliminary studies have projected that the members of the Fortune 500 globally will spend a combined sum of $ 7.8 billion for technical investment, hiring experts and staff training.[4]

The need for additional staff remains one of the most contentious aspects of the new Regulation. GDPR provides that every service which requires 'regular and systematic monitoring of data subjects on a large scale' (Art. 37 GDPR) should designate a data protection officer (DPO) who will ensure the compliance with data protection rules. The interpretation of what constitutes 'large scale' monitoring remains open to interpretation. The Regulation and the later published guidelines on DPOs provides broad examples and guidance on the matter but the final decision whether a DPO should be hired remains up to the company. Given this uncertainty many businesses may opt to hire additional staff as an insurance policy against incompliance. Early estimates suggest that a minimum of 75 000 data protection officers would have to be hired globally in response to GDPR.[5] Of course, we should remain critical of these numbers as they are rough approximations, but a clear point has to be made that GDPR will force a number of global businesses to put additional staff on their payroll.

The potential headache GDPR may cause is not limited to big businesses and multinational companies. Even modest additional expenditure could prove to be precarious for small and medium enterprises and start-ups as they base their business models on lean budgets and limited staff. Every future business plan of an SME would have to calculate additional costs for staff training, necessary software and hardware in order to comply with the new legal framework post 25 May 2018.

For some SMEs, the new rules might mean cutting costs in product development or staff salaries so as to allocate sufficient funds for data protection

Non-compliance is not be an option as the Regulation provides national regulators with the possibility to impose fines up to 20 million euro or 4 % of the company's annual turnover.

Small business faces an additional obstacle by the indirect advantage GDPR gives to big businesses – consumer trust. Established companies and brands operating globally not only have available funds for ensuring compatibility with GDPR but they also have a large number of customers who will be willing to provide their consent for sharing personal data as they recognise and engage with these brands. Under the new

[4] M. Khan, '*Companies face high cost to meet new EU data protection rules',* Financial Times, November 2017, last accessed on 22 May 2018 at: https://goo.gl/UxLP33

[5] R. Heimes and S. Pfeifle, '*Study: GDPR's global reach to require at least 75,000 DPOs worldwide'*, IAPP, November 2016, last accessed on 22 May 2018 at https://goo.gl/qSNCUW

rules, smaller businesses or start-ups developing disruptive innovation will find it more difficult to both invest in GDPR compliance and also gain consumer trust in order to compete with bigger players who are dominating the market when it comes to data accumulation.

Facing uncertainty

The examples above which illustrate the doubts surrounding what actually constitutes valid online consent or whether a company should hire a data protection officer, showcase the spirit of uncertainty surrounding GDPR. Many companies are just not sure what to expect after the Regulation officially enters into force. The lack of established practice or sufficient case law has even rendered legal experts shaky in the advice they provide. Businesses across the globe are expressing their unease and voicing their growing concerns whether they will be sufficiently prepared for the new rules. A pan-European study of business leaders conducted in late 2017 reported that above 90 % of them were still not prepared for GDPR and over half of the respondents agreed that the Regulation is too complex for SMEs and middle market businesses.[6]

A number of companies report hesitance whether they would be fully compliant and are genuinely unsure of what to expect

Most worryingly, some businesses mistakenly expect that there will be a grace period for actual implementation of GDPR and they will have additional time to address specific issues after 25th May 2018.

Many of the member states' administrations are also at unease when it comes to GDPR. The national data protection authorities (DPAs) are crucial when it comes to implementation of the new rules. They are independent public authorities which will supervise the application of GDPR, provide advice, issue warnings and ultimately impose fines for non-compliance. On a supranational level the European Data Protection Board will ensure consistency of GDPR application across the EU and also manage the cooperation between DPAs. This coordinated network should ensure the proper interpretation of the new rules across the member states and make sure that citizens and businesses are treated equally, regardless of their nationality. The reality on the ground, however, is far from desired. In the beginning of 2018 the European Commission reported that only two EU countries are properly prepared for GDPR.[7] This was further confirmed by a recent journalistic survey which reported that at least 17 DPAs across the EU are not prepared for supervising data protection rules properly due to lack of funding, need for additional staff or still lack the full powers to fulfil their duties.[8]

Even though the situation is likely to improve, questions abound about the actual implementation of the new rules. Would DPAs concentrate their efforts on the 'biggest' violators, and would they be able to respond to all citizen complaints in due time?

[6] RSM International, '*92% of European businesses are unprepared for GDPR',* November 2017, last accessed on 23 May 2018 at: https://goo.gl/9M87og

[7] N. Nielsen, '*26 EU states not ready for data law'*, *Euobserver,* 24 January 2018, last accessed on 23 May 2018 at*:* https://euobserver.com/justice/140683

[8] D. Busvine, J. Fioretti and M. Rosemain, '*European regulators: We're not ready for new privacy law',* Reuters news agency, 08 May 2018, last accessed on 22 May 2018: https://goo.gl/1ubWLW

How would an understaffed or underbudgeted DPA approach a GDPR incompliant tech giant?

A series of interpretations of the Regulation are also yet to be provided by data protection authorities (and courts) so that businesses can operate in relative certainty. How effectively would citizens be able to questions the decisions of automatic algorithms which impact them directly? Would GDPR also apply to blockchain or other distributed ledger technology which are based on a system that prima facie is incompliant with the Regulation? Nobody can provide a satisfactory answer at this stage.

The road ahead

GDPR is certainly the right step forward in the effort of regulators to catch up with the digital revolution and provides a positive attempt to safeguard digital rights within the EU. However, it can be argued that the Regulation came late and missed both the rapid expansion of several digital giants, as well as the boom of a myriad of start-ups and new ecosystems across the continent. Because of this tardiness, a number of businesses and especially SMEs would have to go through a painful adjustment to ensure compliance. The EU and specifically data protection authorities will be faced with huge expectations to actually deliver on GDPR and end the painstaking feeling of uncertainty which surrounds the Regulation. The task looks especially challenging given the recent Cambridge Analytica scandal and the ongoing debate on mismanagement of personal data and potential social media regulation.

In the following months we will also see the final developments in the negotiation of the ePrivacy Regulation which aims to complement the GDPR and ensure the confidentiality of electronic communication. The actual implementation of both Regulations will be a litmus test whether European policy-makers can strike a fine balance between guaranteeing user's data protection and electronic privacy while also not imposing tough regulatory burdens on businesses or stifling innovation. This would be a difficult balancing act where the stakes are already quite high. And yet, the European Union has created an unparalleled opportunity. Europe could become the global leader in terms of data protection and have the possibility of exporting this framework to other regions. There have been growing voices from different stakeholders in the US for a more ambitious national legislation in this field. If the EU gets it right, GDPR could serve as a global framework in the future.

Dimitar Lilkov *is Research Officer at the Wilfried Martens Centre for European Studies*

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and likeminded political values.

This publication receives funding from the European Parliament.

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE – 1000

http://www.martenscentre.eu