# May 25, 2018: The end of marketing as we know it?

On May 25, 2016, the EU passed the world's strongest and most far-reaching law aimed at strengthening citizens' fundamental rights in the digital age; simultaneously, the directive also tries to facilitate business by coming up with one set of rules for companies in the EU Digital Single Market. Heretofore, it was up to the individual countries to decide how to implement the tangled web of existing EU laws and recommendations, which made it difficult for enterprises that wanted to do business in multiple countries. This new, 156-page General Data Protection Regulation (GDPR)[1] is something that ALL EU member states voted for unanimously: one law for the entire region. And it comes into force on May 25, 2018 – yes, in less than a year from now!

For the first time ever, the GDPR[2] will apply to any company, organization or body that processes the personal data of any EU citizen, as well as to the transfer of such data. That targets organizations in countries like the US or Russia, which previously could conveniently ignore EU recommendations. Now, if the data is about any EU person, the rules apply. In a Brexit irony, the UK will also have to follow the new regulations whether they're in the EU or not – assuming the data is from an EU person.[3]

In the works since 2012, and with a long history (covered by the first 32 pages of the regulation!), the GDPR seeks to establish a modern and harmonized data protection framework across the EU.[4] Not surprising of such a complex undertaking, some aspects make for quite alarming reading – particularly the parts about the sky-high fines that can be imposed on persons and organizations found guilty of not following the law. This provides fertile ground for fearmongering experts, pundits and vendors – who would all be delighted to sell you products or services to help with compliance.

My nickname – the Father of Customer Intelligence – pretty much gives away which parts of the law I'm most interested in: those that deal with the creation and use of customer data for marketing purposes. And that's why this article is aimed squarely at you as a marketing professional. Because we all, knowingly or not, *create and use EU customer data in the context of our day-to-day marketing activities*.

Before diving in, I think it's important for us in the German-speaking (DACH) world to understand that some of this will just be 'much more of the same.' For about the last 20 years, most EU countries have had data protection laws in force. Many organizations already have the basics in place or are complying with other regulations and standards that overlap the GDPR. For example: in Germany, all companies over 10 employees that collect personal data already need a 'Datenschutzbeauftragter', either as a direct

[1] For general information about the GDPR, see: http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[2] See Article 3.2 of the GDPR. For the complete text (in 24 languages), see: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
[3] http://www.eugdpr.org/gdpr-faqs.html
[4] http://ec.europa.eu/justice/data-protection/reform/index_en.htm

employee or as an external specialist. What will change here with the new law is that the company size differentiation goes away: now every organization – regardless of number of employees – that collects and processes personal data will be required to have this function in place.

**The New "Data Protection Officer"**

What will also change is that, according to Articles 32 through 38, the old Datenschutzbeauftragter will no longer just play an advisory role but will take on the superpowers of a 'Data Protection Officer'; that is, he/she will have the responsibility to gather much more compliance information, define more processes and demand more internal controls than ever before. But good standards and processes around data security and administration already exist; for example, check out the ISO27k Forum,[5] which provides a mapping of the GDPR to the ISO27001 data protection standard[6].

From a marketing perspective, what it immediately means is that the appropriate department at your company should have invited you to participate in discussions and plans. The people doing the inviting will probably have a look of sheer terror in their eyes, as there are so many places within an organization where customer data might be collected and used, and now they have less than a year to sort it out! If you're NOT being asked to participate, *you should be concerned and go talk to your CEO*.

But what, specifically, do marketers need to be aware of? Exactly five topics in the Regulation, three of which are extensions of existing regulations and two that are new! Here, I'll briefly summarize those sections of the law and let you know what you can do to make sure you're not only in compliance but actually leveraging it for your customer (and to your advantage).

**1. Lawfulness of Processing**

Article 6 foresees tighter regulations around gaining personal consent, both when collecting data and when using it. While that will require more work, it's a concept that we in Germany are accustomed to, as the German government – compared to other EU countries (and even closely associated ones like Switzerland) – had already implemented the strictest interpretation of the previous EU data protection law and privacy recommendations.

In my opinion, this is one of the main areas where forward-thinking marketing organizations will be able to shine with GDPR, not just with respect to their customers but also in terms of *creating a competitive advantage*. You ask how? Good! Bend an ear this way…

Anthropologists claim that human societies all share a trait that guides our social thinking: *reciprocity*. I call this concept "give-to-get" in my book:[7] basically, it's trading something of value for something else of value. The private information that belongs to me as an individual is obviously of such great value that it deserves government protection. If data about MY behavior and MY needs is being collected and used without my permission, I might worry about potential abuse thereof. But if an organization tells me not only what data it's collecting on me but why they want to collect it and how its use will positively benefit

[5] See http://www.iso27001security.com/html/forum.html
[6] See http://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx
[7] Customer IMPACT Agenda, Phil Winters, 2017

me as an individual, then I might even agree to it, if I see the value. Think 'information reciprocity.' (You can find seven concrete strategies around this topic in my book!) While my clients have always thought of this as smart marketing, now it's exactly what we need to satisfy the more detailed requirements around data consent. Tell your customers what you're planning to do with their data and why – to help them find what they're looking for, make better recommendations, notify them of important things (such as payments due, software updates, health notifications) or to give them the best price or occasional special offers. And guess what: the better you present it, the more likely they are to see the value and reciprocate by granting you the permission you seek.

Going back to Marketing 101: what's the difference between a new and an existing customer? Data! And the common understanding is that a new customer costs us seven times as much to acquire and keep than an existing one. (I suspect that, in reality, it's much higher.) Keeping this basic premise in mind, I'm suggesting that you dust off your company's boring old Data Privacy Policy and see whether you can read through it without needing a coffee break halfway through. (You're going to have to update it soon anyway!) But what if your company treated this mandatory fine print as *a glossy marketing instrument*? If it were actually attractive, interesting and understandable, and if it presented the topic as a differentiating factor where your customers could clearly see the benefit to themselves, then even you might find the next couple of topics from the GDPR a little less scary!

**2. The Right to Be Informed**

Under Article 12, and further detailed in Article 15, EU citizens have the right to learn exactly what of their data is being collected and how it's being used. And that means the lucky person or team tasked with this must be able to respond quickly and efficiently with information in a "clear and transparent format." For marketing, it means providing those details to the data protection team BEFOREHAND so that they can surface, on request, the required documentation. Although this will mean additional one-time work for us in marketing, once done it should become part of an ongoing process to keep a paper trail on any new data being used or new ways of using existing data. In and of itself, this article of the GDPR doesn't restrict the ways we use data – just how we document that.

Alas, the "clear and transparent format" is still open to interpretation. Article 13 states we need to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[8] Do we need to explain in non-technical terms how our machine learning algorithm came up with a purchase propensity, or why a particular EU citizen didn't get an offer? Some pundits would say yes – virtually ruling out algorithms like "deep learning" and making it very difficult to justify any sort of black box "Artificial Intelligence" approach. But others think explaining the data behind the decision and the decision itself will suffice to fulfill the requirement.

**3. The Right to Erasure**

Another important item in the Regulation will be Article 17, which states that any EU person has the formal "right to be forgotten." This goes far beyond the current regulations, where a person can opt out of being contacted, say, via email. Again, the CPO team must be able to comply with requests within a

[8] GDPR, Article 13, Paragraph 2.(f)

reasonable time frame. Not only for us in marketing but also for all the other departments, this is going to mean working with our CPOs to get processes in place for removing every piece of information – from purchase history to behavioral data (including cookies) to all other data we've legally captured and stored – about a specific person. And every organization, coordinated through its CPO, will need the capacity to quickly provide an extremely detailed description of the data collected – as well as to delete that information – when a citizen asks to be forgotten.

What's interesting here is that, once a person understands exactly what "the right to be forgotten" means, they may never go through with it. After all, who wouldn't want special offers targeted to them (rather than no offers at all)? On a website, they may prefer to be guided to what they're looking for (rather than having to hunt); they may want to be recommended things that are interesting for them (rather than random recommendations); and in general, customers want the organizations they deal with regularly to remember them (purchase history, loyalty, etc.). When the "right to be forgotten" is implemented for an individual, none of that is possible – it's a reset to the zero point. It will be very interesting to see how many people actually invoke this clause once they understand the implications. It all goes back to give-to-get!

**4. Discrimination and Automated Algorithmic Decision Making**

The new area where we as marketing professionals will need to spend the most time and effort with our teams is contained in Article 9 of the GDPR: it's the first piece of legislation to address explicitly the effect of algorithmic decision making on the "fundamental rights and freedoms of natural persons," including *algorithmic discrimination*.

Algorithms are baked into campaign management, marketing automation, CMS and web systems, omni-channel marketing, analytics and predictive analytics: we use machine learning to take the data and figure out a model for predicting an outcome or for categorizing an individual, and then we use that result to take actions. It's most effective when the outcomes are fed back into the system to refine the process for the next time. There's no problem when such machine learning algorithms are applied to the maintenance of machines in a factory or even the pricing of airline seats, but whenever any form of rule-based decision making involves personal data (including cookies and IP addresses), we need to worry about whether 'data that discriminates' has been included in our work.

Discriminatory effects occur when we take decisions around natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation. (Unfortunately, there's also some vague language in the GDPR that states "or that results in measures having such an effect" – meaning unintended discriminatory consequences.) Note that this is true even when we've legally received general permission to collect that data.

So the first step is to identify whether any of the data used in our marketing falls into one of the above categories. This may take a bit of work, but again, it will be a one-time process (along with defining how to make sure we don't actually pick up any more in any new data sources we get in the future).

Do we then simply eliminate the collecting and storing of that kind of data? Absolutely not! Very rarely, there will be an important reason for using the data in our predictive analytics. And we *are* allowed to collect a specific permission for using the potentially discriminatory information for a specific, non-discriminatory purpose.

But the second, perhaps more important, reason to take a different approach has to do with *statistical discrimination*, or the ability of certain types of otherwise 'innocent' data to accurately predict an identified discriminatory topic. A famous case of that comes from the United States, where postal (zip) codes in some regions of the US can be extremely accurate in predicting race. Even if we were to eliminate all indicators of 'race' in our data, the fact that there's a mapping between race and zip code means that we could unknowingly introduce racial discrimination into our models if the proxy known as 'zip code' is available. And, of course, then we might be in violation of the law – for collecting data as necessary and harmless as zip codes! So how do we avoid that?

In the same way we use predictive analytics to do things like determine next best offer or potential to churn, we can use predictive analytics to determine whether the other fields of information we have can predict an identified discriminator. This is something for your data mining teams to do, but at any rate, it should be a well-established process. Once you've documented that there's no problem, you should be good to go.

**5. Anonymity as a Way Forward**

If you read the GDPR in detail, it can sound like a lot of work. However there are two articles that helps us marketers with ways to serve our customers using data: specifically, Article 11, "Processing which does not require identification" and Article 25, which places an emphasis on "pseudonymisation". What that means is that, any time your organization can use truly *anonymous data* in analytic applications, then most of these new rules to notify, provide transparency, etc. (including potential fines for non-compliance) simply *do not apply*. And this is an area of existing expertise that you'll want to take advantage of!

In data mining, anonymous data is data that's impossible to track back to a single individual. There are quick and dirty ways of doing this (such as always using summarized data), but for many of our applications (risk, upsell, cross-sell, recommendation, etc.) that degree of consolidation will remove the detail we need to create accurate predictive models. However, there are advanced techniques around that we can exploit. They've been around for years in the pharmaceuticals industry, for example to anonymize the patient data from clinical trials required to get new drugs approved. I myself am now working with a number of open source organizations to make it easier to understand and use these techniques. I will be sharing them in the coming months.

You should expect your data mining team to want to talk with you about these topics in the coming months because it gives us exactly what we need: the ability to let customer data guide and support business activities in a fully compliant way.

I see the GDPR regulations as a positive step forward. Yes, initially it will mean work for our organizations, but in the end it will provide us with plenty of opportunities to shine while doing what it was designed to do: **protect natural persons with regard to the processing of their personal data while restricting the unauthorized movement of that data.**