DMN DATA. STRATEGY. TECHNOLOGY.

SPONSORED BY melissa mailjet

THE DEFINITIVE GUIDE TO

HOW BRANDS CAN PREPARE FOR COMPLIANCE

Hillary Adler
Senior Editor
DMN

TABLE OF CONTENTS

If you work with data, or if data is important to your brand, you've no doubt heard about GDPR. The General Data Protection Regulation is a piece of legislation which will come into force across the European Union on May 25, 2018.

But you shouldn't turn your head the other way even if you're an American company. GDPR will affect your brand if your marketing and eCommerce operations reach a European audience.

For companies who operate in European markets or who have actual or potential customers within those countries — even if your physical operations take place in the United States — strict compliance with GDPR is mandatory, and the penalty for failing to comply is a fine.

A major fine.

We're talking about a 4 percent of your global annual revenue (or up to €20 Million) kind of fine.

In short, if you process data about individuals in the context of selling goods or services to European citizens in any EU country, then you will need to comply with GDPR.

But what exactly does GDPR require, and how must you comply?

WHAT GDPR MEANS FOR U.S. BRANDS

By Hillary Adler, Senior Editor, DMN

At the bare minimum, the GDPR was drafted with the intended purposes of protecting all non-anonymized personal data (or personally identifiable information: PII). Any company (or organization) that stores or processes personal information about "natural persons" (individual human beings) who are "data subjects" under the Regulation — defined as European citizens who reside in an EU state — must comply.

THE BASICS OF GDPR: A BREAKDOWN

In its long and detailed text, the GDPR defines what types of personal data are at stake:

- Name, address, and phone number
- IP address and cookies
- Racial identity
- Religious and religious affiliation
- Health and genetic data
- Biometric data
- Sexual orientation and gender preference

WHAT MATTERS TO DIGITAL MARKETERS

Storing or processing of personal data can be undertaken only if:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data; in particular where the data subject is a child.

It's a lot of legalese, I know. So to put it in layman's terms: You can't just go ahead and profit from personal data anymore, if the data relates to European data subjects. Maybe we should just quote paragraph 70 of the preamble to underline that point — emphasis added:

"Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information."

NAVIGATING GDPR: DATA CONTROLLERS AND DATA PROCESSORS

On the one hand, this imperative to protect personally identifiable information about European subjects threatens business strategies, practices, and processes worldwide, especially cloud, SaaS, and mobile-driven enterprises. In order to cope with the GDPR, brands with international operations have been developing alternative and compliant data-storage centers within the EU.

32%
of respondents plan to reduce their presence in Europe.

According to a report released by PwC, 64% of executives at U.S. corporations reported that "their top strategy for reducing GDPR exposure is centralization of data centers in Europe. Just over half (54%) said they plan to de-identify [i.e. anonymize] European personal data to reduce exposure."

26%
Intend to exit the EU market altogether.

"The threats of high fines and impactful injunctions, however, clearly have many others reconsidering the importance of the European market," the study says. In fact, 32% of respondents plan to reduce their presence in Europe, while 26% intend to exit the EU market altogether.

That's a high percentage of lost business, but if you're a company who wants to navigate the terrain and remain in the EU, here are a few things you need to think about.

WHETHER YOU'RE A DATA CONTROLLER OR DATA PROCESSOR (OR BOTH)

According to Article 4 of Regulation, these two roles are distinguished as follows:

- **A Data Controller is:** "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data..."
- **A Data Processor is:** "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."
- **What it means:** This marks a departure from previous European data law, which affected only controllers, not processors working for them. If it's not obvious, brands offering products or services are likely going to find themselves under "other body" in those definitions.

Whether you need to designate a Data Protection Officer

Some controllers — and processors — will be required to designate a Data Protection Officer (DPO). In addition to being mandatory for public authorities, any company involved in "regular and systematic monitoring of data subjects on a large scale," or if its "core activities" involve large-scale processing of particularly sensitive data (such as data relating to someone's racial or ethnic origin, religious or political affiliation, health, sexual preference or criminal history) will need a DPO.

This seems to apply to any United States-based brand whose marketing or sales operations involve large-scale processing of non-anonymized data, including information about European data subjects. The DPO can be a contractor, but must possess the requisite specialist knowledge. EU-issued guidelines recommend that the DPO be located in a members' country and report directly to senior management.

SAFEGUARDING ADDITIONAL DATA SUBJECT RIGHTS

According to Article 12 of the GDPR, THE DATA SUBJECT ALSO HAS OTHER IMPORTANT RIGHTS, INCLUDING:

- **Access:** The right, exercised at reasonable intervals, to know what personal data has been collected and how such data has been processed
- **Accuracy:** The right to restrict processing where data is inaccurate
- **Consent:** The data subject's "freely given" and "explicit" consent to the processing and storage of personal data must be sought in "clear and plain language," separate from other information. Significantly, consent may not be regarded as "freely given," where performance of a contract is made conditional on consent, where that consent is unnecessary to the performance of that contract. This has the potential to restrict fishing for personal data in eCommerce contexts. *(Also, while existing consents may be adequate, they should be audited to ensure they meet these new conditions.)*
- **Data Portability:** The right to request and receive their personal data from a controller in a format which allows it easily to be transferred to another data controller.
- **Erasure (right to be forgotten):** The subject has the right to withdraw consent and ask for personal data to be "erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her..." *(paragraph 65 of the preamble).*

Other provisions you need to watch

There are many layers of detail beneath the complicated-enough terrain. For example, GDPR allows transfer of data across borders in various circumstances, including a finding that the destination territory can adequately protect the data.

Since the demise of the "safe harbor" agreement, it's not clear that the United States (or Canada) meets that standard, except partially. There is an opportunity to conduct legitimate intra-group data transfers under a system of "Binding Corporate Rules," where members of joint commercial enterprises confer legally enforceable rights on data subjects to have their data protected when transferred internationally.

Still not convinced GDPR will change the way your brand does business? Remember, we are not lawyers. We can lay the information out to the best of our ability, but if you think you might be affected, it's time to seek expert advice.

GDPR: WHAT MATTERS TO CONSUMERS

By Kim Davis, Editor-in-Chief, DMN

"It's not an EU regulation which just affects businesses in the EU. It affects EU residents."

That's what Jeff Nicholson, VP of CRM product marketing at Pega told me. It goes right to the very heart of why GDPR is different, and why it requires the focused attention of brands and brand marketers — not just in Europe, but around the world.

"For the longest time," said Nicholson, "customer data has been thought of as a corporate asset. This turns it on its head." For the personal data of European data subjects, "this changes the entire dynamic."

A wake-up call for U.S. brands

Pega, the veteran BPM/CRM platform, is headquartered in Boston, but has a global footprint. As for the EU, "We're across the region," said Nicholson, with offices in the Benelux, France, Germany, Italy, Poland, and Sweden.

This puts Pega on the front line when it comes to understanding GDPR, and providing advice on compliance. Do U.S. brands get it yet?

"They're slowly waking up to this new reality they have to come to grips with," said Nicholson. "They need to devise a strategy to comply. If someone filled out a web form — a year ago, or yesterday — maybe they were applying for a line of credit — you have their data." Of course, we're talking about the personal data of European data subjects. What if I market products and services to the U.S., and just happen to have collected some European data by accident: Do I have exposure?

"Technically yes," said Nicholson, "but you have to ask yourself to what extent you're at the risk of someone enacting a GDPR request."

"They need to devise a strategy to comply. If someone filled out a web form — a year ago, or yesterday — maybe they were applying for a line of credit — you have their data."

— Jeff Nicholson, VP of CRM product marketing, Pega

Make no mistake, brands which are conducting eCommerce across borders as a matter of routine are certainly affected.

What will trigger GDPR requests?

Part and parcel of putting data ownership squarely in the hands of individual consumers, is that it's the consumers which can trigger problems for unprepared brands. European data subjects have multiple rights under GDPR — not just to have their consent to collect data clearly sought, but to have data corrected, erased, or returned to them. In some respects, this triggered a false sense of security among brands, with the majority of consumers not seeming to care much — or understand much — about the Regulation.

This is where Pega saw an opportunity. Among the many surveys asking if brands were prepared to comply, there was an absence of data on how consumers were likely to respond. To fill the gap, Pega surveyed 7,000 consumers in seven EU countries (an enormous consumer survey by any standard). This is what they found:

While only 21% of those surveyed understood their rights under GDPR:

- **90%** want direct control over how companies use their data
- **89%** want to see the data companies store on them
- **47%** see the latter as their most important right
- **22%** see the ability to have their data erased as their most important right, and
- **45%** say that finding their data had been sold or shared would be the biggest motivation for a GDPR request.

In other words, once consumers are informed about GDPR, look out.

>>>

POTENTIAL PENALTY FOR GDPR VIOLATIONS:
4 PERCENT OF GLOBAL ANNUAL REVENUE (OR UP TO €20 MILLION)

Brand behavior can trigger problems

Given the history of data activism in Europe, it seems likely that an attempt to make an example of a high-profile brand by launching onerous GDPR requests is surely inevitable. And that will put GDPR in the news and encourage further requests. "It's likely to happen," Nicholson agreed. "But will it be just a circus act, or something which really has an impact? But yes, someone will try to test the system at some point."

"But yes, someone will try to test the system at some point."

All it takes, he said, is a tweet by someone with millions of followers identifying a brand as a target.

The imperative brands should take away from this data, Nicholson explained, is that "they need to build a new skill set they probably don't have today. They need to anticipate behaviors which might trigger these requests, and avert them before they happen."

melissa

PARTNER PERSPECTIVE

"Our responsibility now runs even deeper and we'll need to work even harder to put the customer first, especially in the areas of customer onboarding and subsequent marketing for legitimate business interest."

– Greg Brown, VP, Marketing, Melissa

Consumers who are subjected to intrusive, irrelevant messaging are going to be concerned about what data is out there and how it's being used. This is a serious matter for brands, beyond the threat of fines. Data, Nicholson said, is basic fuel for many marketers; if data is erased, lines of communication with that customer are cut.

The challenge, he said, "is to understand not only data, but what matters." Some of the data brands are using now, without proper permissions or accuracy checks, is "shallow" anyway. Take away the kind of data-based marketing which isn't of interest to consumers and "you're saving money, you're limiting marketing fatigue."

And maybe, under GDPR, you're keeping communications alive.

GDPR LEGISLATION TIMELINE

Oct. 24, 1995: Data Protection Directive 95/46/EC created to regulate the processing of personal data

Jan. 25, 2012: European Commission releases initial proposal for updated data protection regulation

Mar. 12, 2014: European Parliament approves version of regulation in first reading

June 15, 2015: Council of European Union approves version in its "first reading," allowing measure to pass into final legislative stage (also know as the "Trilogue"

Dec. 15, 2015: European Parliament and Council agree on proposed GDPR legislation, official signing set for January 2016

Apr. 8, 2016: Legislation adopted by the Council of the EU

Apr. 16, 2016: Legislation adopted by European Parliament

May 2016: Regulation "enters into force" 20 days after entrance into EU Official Journal

May 25, 2018: GDPR becomes fully enforceable throughout EU after a two-year post-adoption period

EUGDPR.org

COOKIES AND CONSENT: HOW GDPR IMPACTS ONLINE TRACKING

By Amy Onorato, Special Projects Editor, DMN

For marketers, the biggest GDPR concerns surround the issue of data collection and consent

Organizations that collect personal data from European data subjects need to start paying attention to how GDPR will impact their general business practices, and evaluate their need for compliance.

For marketers, the biggest concerns surround the issue of data collection and consent. Online, one of the most common ways of collecting data is through "cookies," or small packets of data left by websites on web browsers.

Privacy concerns surrounding cookies has been an issue for several years now. Under GDPR, it's important to understand that personal data, like IP addresses and other information collected by cookies, is not a corporate asset, but is owned by the data subject.

Here's a breakdown of what you need to know:

How does GDPR impact cookies and consent?

Privacy concerns surrounding cookies aren't new in the EU. Regulations surrounding cookies and consent were first adopted in 2011. As Guillaume Marcerou, Criteo global privacy director, wrote:

"One of the most discussed issues for the digital marketing industry is that technical identifiers such as Cookies and Mobile Advertising IDs are now considered personal data. While this may seem like an exceptional development to many US-based companies subject to the regulation, this was already the case in many EU countries, including France."

Here's what's different. Under GDPR, "all EU member states must treat cookies and other technical identifiers as personal data."

Parties who violate these regulations will now also be subject to penalties, which could amount to as much as 4 percent of global annual revenue, or a €20 Million fine, whichever is greater. U.S. companies that collect the personal data of European data subjects must comply with the new rule.

WHAT ARE COOKIES?

Cookies are pieces of tracking data which are placed by websites on a user's browser. They serve a number of different purposes. For example, websites might use cookies to track:

- **Whether a user is logged into an account**
- **Whether they've added or removed items from their shopping cart**
- **To track browser history (to create more personalized user experiences)**

Cookies can also be used by third parties to track user browsing history. Common third-party use cases include advertisers who want to track traffic from ads placed on other websites.

Asking for consent under GDPR

To be compliant, organizations must ensure consent for processing and storage of personal data is "freely given," with that consent sought in "clear and plain language."

Request for consent is not regarded as "freely given" if it is granted under conditional terms, or as a conditional provision where consent is not critical to the "performance of the contract."

"What you need to do is make sure you are providing a comprehensive cookie notice," Marcerou said in an interview.

Simply put, this means brands must explicitly educate users on how they plan to use their personal data, on an opt-in basis. Organizations also can't restrict website usability or services based on whether consent was granted.

"Publishers will still have to make their content available," Doug McPherson, chief administrative officer and general counsel at OpenX, a programmatic advertising company, said.

Consent is not required for cookies that are used specifically for the collection of "non-sensitive personal data" – like a cookie that is used to track items in a user's shopping cart. However, if a cookie collects any personal data, which, under GDPR, includes IP addresses that are tied to users, this could be considered an infringement on regulation and subject to penalty.

Though third-party cookies are not owned by the sites they are dropped on, companies that allow these cookies can still be held liable for violations associated with data collection.

"In general, a website owner can be held liable for GDPR violations by a third party that is collecting EU personal data by dropping pixels," McPherson said.

> ***If a cookie collects any personal data, which, under GDPR, includes IP addresses that are tied to users, this could be considered an infringement on regulation and subject to penalty.***

TO REMAIN COMPLIANT, COMPANIES MUST ENSURE THAT PERSONAL DATA OR OTHER IDENTIFIERS ARE ONLY COLLECTED AFTER A USER EXPRESSES CONSENT.

When to ask for consent

Under GDPR, it is imperative for organizations who distribute cookies to allow users to express consent before the cookie is dropped. In many cases, cookies are dropped upon a user's arrival at a website to track attribution. This could a problem for companies under GDPR.

"Even if the user refuses the user cookie, the cookie is already dropped and the cookie is already tracked," Marcerou said.

To remain compliant, companies must ensure that personal data or other identifiers are only collected after a user expresses consent. This can be done by launching an opt-in banner immediately a user enters the site. Brands should also make their privacy policy clear and accessible to users.

"Clear consent must derive from the use of the cookie for a specific purpose," Marcerou said.

Despite these apparent restrictions, Marcerou says the breadth of the GDPR directive is actually intended to create a more unifying body of laws regarding data privacy: "To ensure a free flow of data across the member states," Marcerou said.

>>>

A CLOSER LOOK: IS GATED CONTENT THE SOLUTION?

By Kim Davis, Editor-in-Chief, DMN

Brands want to know how to collect personal data from European data subjects under the restrictions imposed by GDPR. Many have said that creating gated content — content which requires completion of form to view — is a solution.

We're not so sure.

The relevant constraints here are that a consumer's consent to the collection of data must be "freely given" and "explicit," and must be sought in "clear and plain language," and "separately from any other information."

So far, so good. Let's say a pop-up, a lightbox, or whatever kind of form a website uses, is clear and unambiguous about its request for personal information. The user is required to complete the form to earn access to a whitepaper, a webcast, a video, or some other web content.

All good? Many seem to think so. Scott Brinker, a reliable source on all things martech writes:

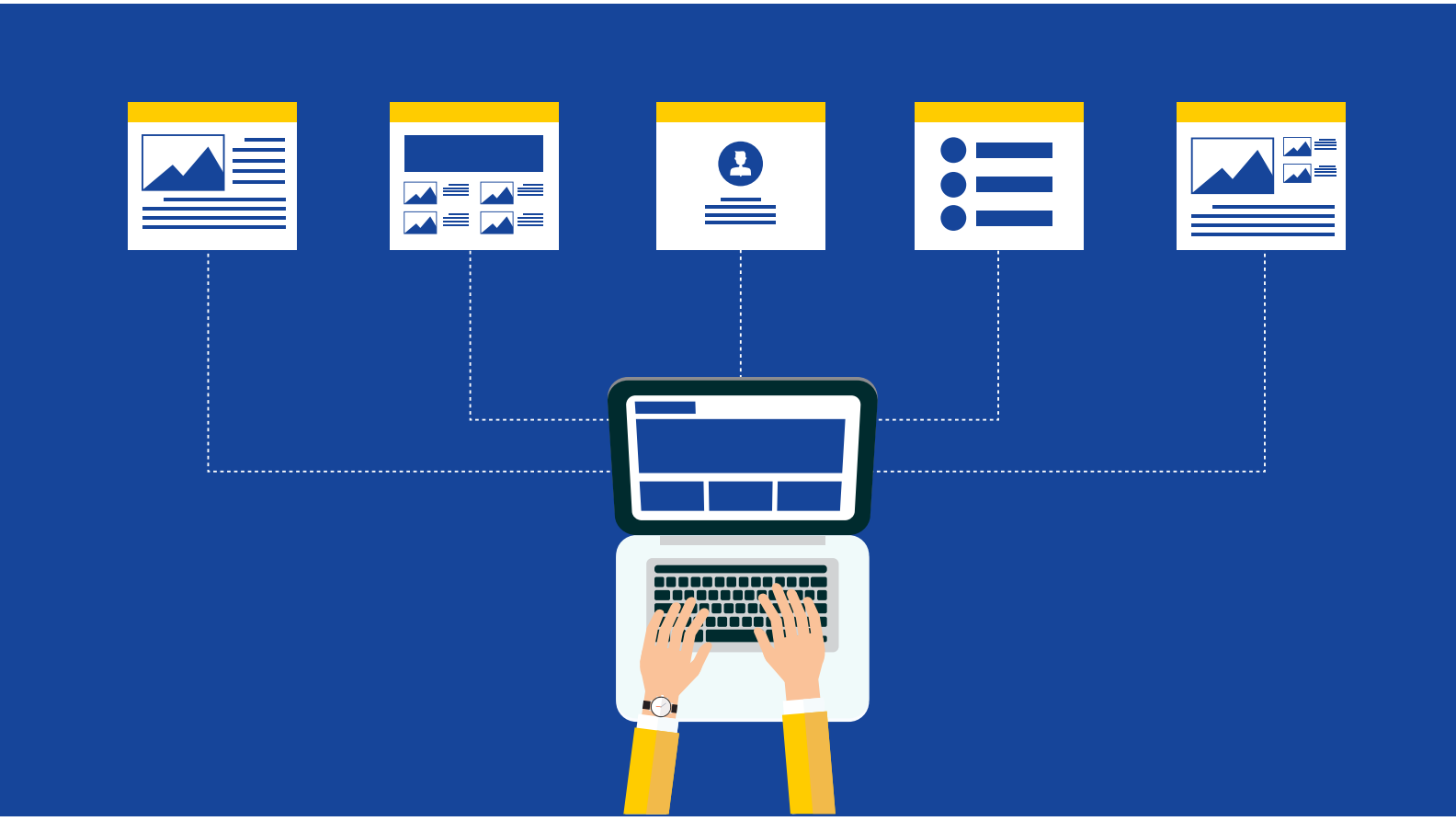
"To encourage users to subscribe or opt in to specific types of content — versus an all-or-nothing approach — marketers should build preference centers, enabling clients to control how they prefer to engage with you. For example, clients may opt out of general marketing emails, but opt in to event invitations. Marketers should focus on tactics like gated content, website subscription pop-ups and event subscriptions."

Hubspot, via the B2B Marketing Lab, proposes:

"As you attract these individuals, you convert them into leads using forms, calls-to-action and landing pages on your website using high-quality 'gated content.' Throughout the inbound process, every exchange has been consensual and can be easily tracked..."

But is the situation really that clear? Consider the language in Article 7, "Conditions for Consent:"

"When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."



melissa

PARTNER PERSPECTIVE

"Brands need to assess and monitor their data vendors and partners to ensure they are handling and processing their data consistent with GDPR regulation. Finding every related record within every databases is a problem that every organization should be addressing now – both internally and with outside help."

– Greg Brown, VP, Marketing, Melissa

In lay terms, the language seems to say that consent is not freely given if the data subject can't get a contract performed or a service provided without offering up their data, where the data isn't necessary to performing the contract or providing the service.

Now, whatever marketers might think, collecting personal data just isn't a necessary precondition of reading a whitepaper or viewing a video. We are not lawyers (as we always insist), but a contract usually implies exchange of value between two parties. Maybe this provision only applies where a data subject is paying to register to read, view, or attend some piece of content? Perhaps the data collection is necessary to process payment and record the registration?

Perhaps. But at the very least, Article 7 does seem to place a burden on the data processor to show that it was necessary to collect personal data before the data subject could be allowed access to the content. That may be a high hurdle if no fee is being collected (and credit card details, etc., required), or the brand is not explicitly asking the subject to join a mailing list —or perhaps become a registered member of a community.

After all, what the form usually means is: "Here's a piece of content you can only consume on condition you hand over your personal data, which I am going to store and use to try to sell you stuff." And to say the least, that goes against the spirit of "freely-given" consent.

After all, if consumers are going to be given the option to click on: "No thanks, I don't want to give you my data," and get access to the content anyway, the so-called gate is wide open.

GDPR AND CHILDREN'S DATA:

WHAT BRANDS NEED TO KNOW

By Amy Onorato, Special Projects Editor, DMN

Collecting data from children is already subject to legislation in the United States. But as GDPR comes into effect, there are certain provisions brands that work with children's data need to pay attention to

Under GDPR, "processing of the personal data of a child" is only allowed by law when the child is at least 16 years old. If a child is under 16 years of age, companies must obtain consent from the child's parent or legal guardian to collect and process their data. Any collection of data from children under the age of 13 is prohibited.

> ***It's not just making the copy appropriate for general audiences – it's for an audience that may not have as clear of an understanding of their rights.***

The United States' current Children's Online Privacy Protection rule (COPPA) allows for organizations to begin collecting data without parental consent at age 13. This means that brands collecting data may need to expand their current consent obligations to include children up to age 16.

Parental consent

Brands who seek consent must also "make reasonable efforts" to verify that parental consent is valid. However, it does not explicitly state how organizations are supposed to do this; only that it must be done by "taking into consideration available technology."

Notably, GDPR also states that any privacy notice from organizations looking to collect data directly from a child must write their privacy notice in a way that is clear and easy to understand for children:

> ***"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."***
> (Recital 58 EU GDPR)

This is where some brands need to take notice, and another look, at how their privacy policies are worded. In general, privacy policies need to be written in such a way that makes them accessible to potential users – which can already be a challenge if jargon and legalese is used.

Brands need to consider how certain policies are explained when speaking to a child. In these use cases, it's not just making the copy appropriate for general audiences – it's for an audience that may not have as clear of an understanding of their rights.

"AS A POLICY, WE WORK TO 'PROTECT' OUR AUDIENCES, RATHER THAN SIMPLY ABIDING BY LAWS AND RULES."

Paul Beck, CMO, Storybooth

Protection of data

Generally, GDPR stresses the importance of clarification when data collection is being used for the purpose of marketing or advertising:

"This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."
(Recital 58 EU GDPR)

In the United States, there are already measures that organizations collecting data from children need to follow to protect children from third-parties that may not have as stringent policies in place.

Keeping advertisers at 'arm's distance'

Storybooth, a company that turns user-submitted stories into animated YouTube videos, regularly collects data from minors.

"We have an extremely hard line against third parties getting access to them through what we can control," Paul Beck, CMO, said. "We do not allow third parties to engage with them directly on our channels where we can control it."

"As a policy, we work to 'protect' our audiences, rather than simply abiding by laws and rules," Beck continued. "We have checks and balances set up to ensure we stay 'arms distance,' protecting them from third-party access to our audience."

SAP HYBRIS: A THREE-PART STRATEGY FOR GDPR

By Kim Davis, Editor-in-Chief, DMN

I wanted to give SAP Hybris a voice in the GDPR discussion, because of their deep European roots in the business. But that's not the only valuable perspective Hybris brings. It also brings the customer identity smarts of Gigya, which joined the SAP stable in September 2017. I spoke with Patrick Salyer, Gigya's long-time CEO.

"There's an over-arching mega-trend that GDPR is part of," Salyer said. "Consumers want a great customer experience — we get that — but consumers want it done the right way. They're tired of creepy experiences where they don't know what's happening to their data, or if they're being tracked without their knowledge. There's a real push back, and a demand for transparency and control."

Three new solutions make up the Gigya-driven response to this new environment: **Identity**, **Consent**, and **Profile**.

"It really begins with SAP Hybris identity," Salyer explained. "As a starting point, you need to know who someone is."

This means deterministic self-identification, through authentication or registration (for example via social log in or Touch ID). Second, and described by Salyer as "the core" of the GDPR offering, is SAP Hybris Consent.

"You need to get [user] permission to access their information and market to them, and to give them control and transparency around that," he said.

For brands, that means managing terms of service to consumers, tied to privacy policy, and getting re-consent when terms of service change. It also means giving users controls to opt into "certain marketing or personalization efforts," and to view, delete, or export their profiles.

> ***"Consumers want a great customer experience — we get that — but consumers want it done the right way."***
> Patrick Salyer, CEO, Gigya

Adding complexity, some brands will need to manage these processes consistently across hundreds of web pages and apps. They'll also be compelled to go back over historic data to see what existing customers have consented to.

Finally, there's the obligation to manage the profile itself. It's a particularly sharp challenge given the plethora of downstream marketing and sales applications which need to not only access data about an individual consumer, but understand what permissions they have — or don't have — to use that data.

"A really simple email marketing tool usually has its own storage of customer data, but does it know if it has the latest data? Does it have the right to email that user, once a week or once a month? You really need to store the information at a central location — and that is Profile," Salyer said.

> ***"A really simple email marketing tool usually has its own storage of customer data, but does it know if it has the latest data?"***
> —Patrick Salyer, CEO, Gigya

Given Gigya's core competency in customer identity management, I wondered if the SAP acquisition had GDPR or similar regulatory regimes in mind.

"I think SAP in general is a company which knows the importance of trusted relationships," Salyer said. "I also think it's a privacy-minded brand when it comes to software, especially given its European roots. They've understood this trend for a long time; they saw the importance of GDPR compliance coming on the horizon. For us at Gigya, it just made a fantastic fit."

The reaction of European brands to the approach of GDPR seemed much more positive than that of their North American counterparts. Marketers seemed to relish the promise of clean, reliable, permission-based personal data. Salyer agreed.

"I'm hearing that more and more from our customers and prospects. To be honest, you're starting to see a shift in the last six months that it's not just in Europe. Others are catching on, specifically in North America. For the last ten years we've driven personalization, but we've done it by using data without permission; and that data is really, really inaccurate. It just is."

>>>

GDPR: WHY MARKETERS SHOULD LOVE IT

By Joe Stanganelli, principal, Beacon Hill Law

Naturally, people are preparing for the worst. But GDPR can be your edge

The marketers I know tend to fall into one of four categories when it comes to preparedness for the European Union's General Data Protection Regulation (GDPR):

The fretful: "I'm going to screw things up under GDPR. Oh, no!"

The resigned: "I'm going to screw things up under GDPR. Oh, well!"

The ignorant: "What's GDPR?"

The apathetic: "Boring!"

I'm here to urge you be a fifth type, **the eager**: "GDPR is coming! Oh, boy!"

You read that right.

As we've discussed, organizations that collect and/or maintain the data of EU "data subjects" (a vague term) may face severe fines if they fail to adhere to strict rules governing how they can collect relevant data — and what they can, must, and mustn't do with said data.

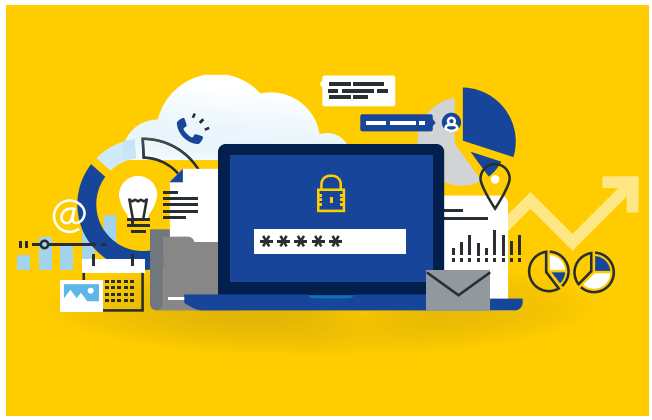
Emphasis on "strict." GDPR is perhaps the most far-reaching and complex data regulatory framework ever (not that that's saying a lot). Moreover, it may not even be applied consistently, because different member states will have a certain degree of autonomy in interpreting and enforcing it.

THINK OF IT AS "YOU GET TO MAKE DATA PRIVACY A FEATURE OF YOUR BRAND."

Naturally, people are preparing for the worst. But GDPR can be your edge. What's a marketer to do (beyond try to get in and out of the company lawyer's office without getting talked to death)?

Effectively, be a better marketer.

The lawyer's way of looking at GDPR is "you have to do this" — because lawyers are straightforward pessimists. But you're a marketer — stereotypically, an imaginative optimist. Think of it as "you get to make data privacy a feature of your brand."



While other marketers will be doing their utmost to undercut their data officer's demands and engage in bare-minimum, check-the-box compliance, you have a unique opportunity to boast about the measures you take to protect — and respect — data.

YOU HAVE A UNIQUE OPPORTUNITY TO BOAST ABOUT THE MEASURES YOU TAKE TO PROTECT — AND RESPECT — DATA.

While other marketers will be huffing and puffing just to make sure that their inbound strategies aren't too dinged up by in-house counsel, you can use your marketing playbook to solve the legal problem by treating "explicit consent" as your latest product. From there, you can strategize how to market it accordingly to both new and pre-existing customers at each touchpoint.

Most importantly, while other marketers are throwing up their hands in frustration, you'll be enjoying GDPR enlightenment.

>>>

GDPR MEANS NEVER HAVING TO SAY "GOTCHA!"

The fundamental precept of GDPR is that you're going to have to stop doing sleazy marketer stuff.

Of course, you don't do sleazy marketer stuff — and I would never accuse you of doing so. But you probably have some marketer colleagues who do. So let's talk about them, your offshoot underachievers — or "you" for short.

For instance, you know how you sometimes "helpfully" pre-tick opt-in boxes for website visitors, or use similar tactics to "fool" people into sharing data with no strings attached?

That's a big no-no where GDPR compliance is concerned.

Here are pretty much the only things you are accomplishing with these shenanigans:

1. You sign people up for things they don't want, leading some of them to attempt to unsubscribe themselves.

The result: Twofold. First, to some degree (albeit likely a small degree), you will spend (waste) resources accommodating people as they try to reverse what you tricked them into doing.

Second, and more importantly, you suffer automatic brand damage for each one of these malcontents. Even if they aren't a qualified lead, consumers may well spread their tales of woe about the hassle you have caused them.

2. You are getting other people signed up for things they don't really want, leading some of them to suffer through the consequences without having the ability to unwind what's happened to them.

The result: In the attempts to beat someone into becoming a lead, you have given birth to a distinct segment of people who hate you and are frequently reminded of exactly why they hate you.

3. You are causing yet another person to have to take a preemptive action to avoid the trap you set.

The result: Again, cumulative brand damage with each eyeroll and sigh you cause. Worse yet, persnickety people multiply the effects of negative word of mouth.

4. You are artificially inflating the marketing team's engagement numbers with people who didn't mean to take the action.

The result: Whatever engagement you are trying to achieve becomes a vanity metric, negatively skewing the organization's ability to effectively draw the correct actionable insights in the future.

In the end, in addition to giving you new opportunities, GDPR compliance will protect you from yourself. You will have to do grown-up marketer things like strategizing, analyzing qualified leads, determining and tracking KPIs, targeting, and managing your campaigns on an ongoing basis.

Effectively, GDPR will force you to be great at your job. So why not start now?

13 KEY GDPR TERMS YOU NEED TO KNOW

01

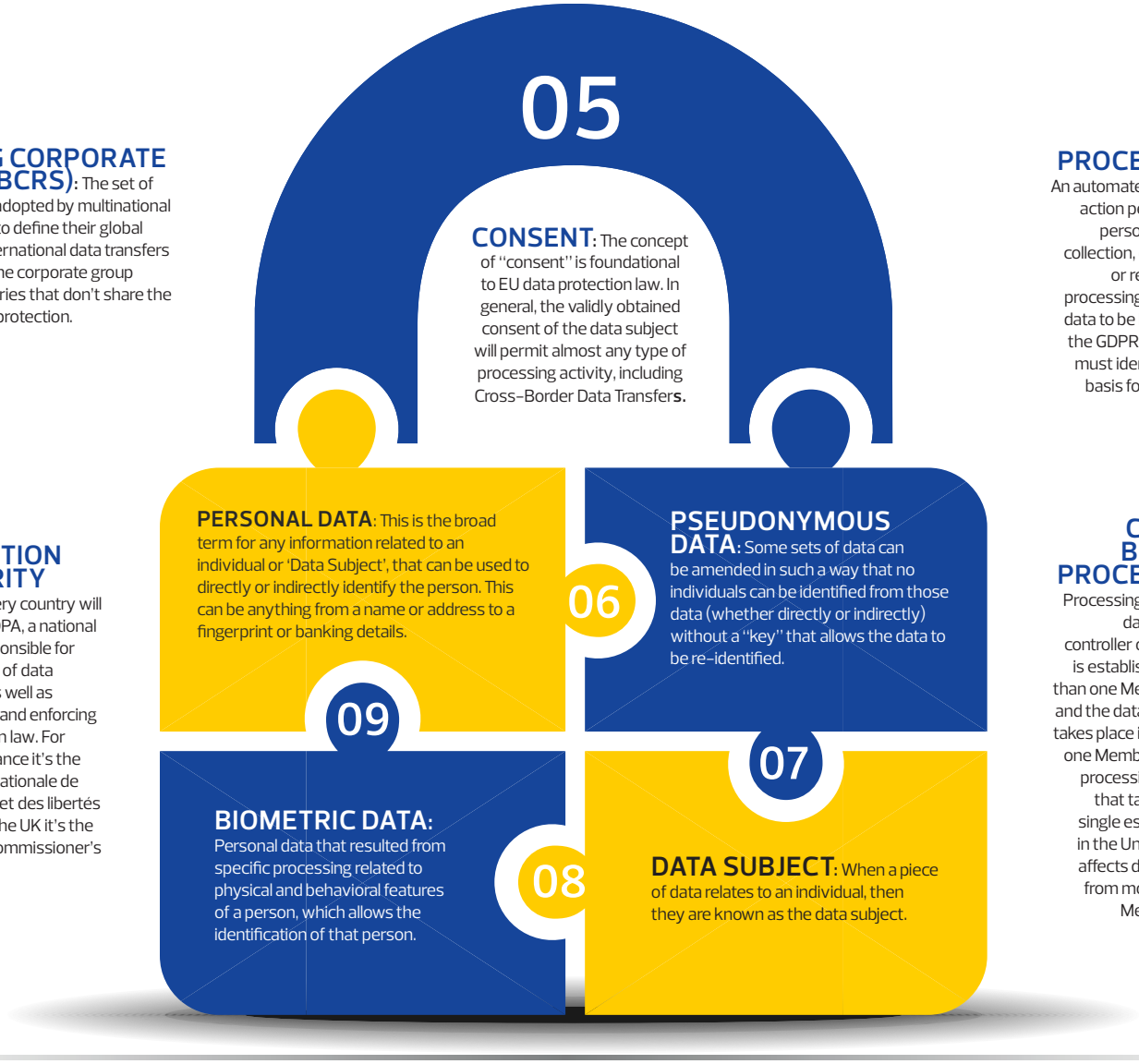
BINDING CORPORATE RULES (BCRS): The set of internal rules adopted by multinational companies in to define their global policies on international data transfers within the same corporate group towards countries that don't share the same level of protection.

02

PROCESSING: An automated or manual action performed on personal data, like collection, organization or recording. For processing of personal data to be lawful under the GDPR, businesses must identify a lawful basis for this action.

03

DATA PROTECTION AUTHORITY (DPA): Every country will have its own DPA, a national authority responsible for the protection of data and privacy as well as implementing and enforcing data protection law. For example, in France it's the Commission nationale de l'informatique et des libertés (CNIL) and in the UK it's the Information Commissioner's Office (ICO).



04

CROSS-BORDER PROCESSING: Processing of personal data when the controller or processor is established in more than one Member State, and the data processing takes place in more than one Member State, OR processing activities that take place in a single establishment in the Union, but that affects data subjects from more than one Member State.

10

DATA CONTROLLER: Like the existing Data Protection Act (DPA), the GDPR applies to Data Controllers who process personal data. So first, who is the Data Controller? This is a person who decides the purpose for which any personal data is to be processed and the way in which it is to be processed. This can be decided by one person alone or jointly with other people.

11

DATA PROCESSOR: Unlike the DPA, the GDPR introduces specific responsibilities for the Data Processor. These are third parties that process data on behalf of the Data Controller and includes IT service providers.

12

DATA PROTECTION OFFICER: A Data Protection Officer is someone who is given formal responsibility for data protection compliance within a business. Not every business will need to appoint a data protection officer – you need to do so if:

- Your organization is a public authority; or
- You carry out large-scale systematic monitoring of individuals (for example, online behavior tracking); or
- You carry out large-scale processing of special categories of data or data relating to criminal convictions and offenses.

13

RIGHT TO BE FORGOTTEN: The right to erasure of personal data or 'the right to be forgotten' enables an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing

>>>

Is Your Marketing Data GDPR Ready?

GDPR is right around the corner. It will impact marketers who deal with customers and prospects who are EU citizens. Melissa can help you make the change and ensure your marketing is reliable and sustainable.

- Risk Assessment Audit & Matching Gap Analysis
- Data Cleanse & Dedupe
- Data Enrichment: Missing Country/Job Title & Social Media
- Contact Discover: B2B & B2C

Whether you're looking to build a custom prospect database or cleanse your existing customer file – we have the best data quality and compliant data available.

Get a Single Customer View Audit Now!

Learn more at Melissa.com

1-800-MELISSA

melissa

DMN DATA. STRATEGY. TECHNOLOGY.

YOUR GO-TO SOURCE FOR THE LATEST DIGITAL AND DATA-DRIVEN MARKETING TRENDS.

NEWSLETTERS

DMN Daily Insider

A must-read for breaking news coverage and expert analysis on all aspects of marketing.

DMN Best Of...Weekly

Hitting inboxes every Friday, Best Of...Weekly highlights the week's top DMN articles (in case you missed anything!)

DMNTech Roundup

A weekly update on marketing technology, data and innovation from DMNTech.

Subscribe to any of our newsletters at DMNews.com/newsletters

DMNews.com

Data. Strategy. Marketing technology. Everything you need to do your job well.

@dmnews

dmnews.com/linkedin

facebook.com/directmarketingnews