The Burdens and Benefits of the GDPR:
A Practical Guide for Marketers

BY TIM WALTERS, PHD

SPONSORED BY

Lytics

About This Report

This introduction to the General Data Protection Regulation (GDPR) is intended to provide marketers and related roles with an initial sense of their obligations and opportunities under this new regulation. This orientation is delivered in the form of a conversational FAQ. While by no means comprehensive, the FAQ aims to cover both the most common and the most essential questions about the GDPR for marketers. Sidebars and graphics provide additional information about terminology, key provisions of the regulation, and so forth.

The FAQ is organized into the following sections:

- **The basics:** What is the GDPR and what does it want from me?
- **Consent:** Obtaining permission to use personal data
- **Legitimate interest:** A get-out-of-jail-free card for marketers under the GDPR?
- **The data subject rights:** Putting consumers in control of their data
- **Accountability:** Proving that you are compliant with the GDPR
- **Other considerations:** The parts of the GDPR we're not talking about in detail: data security, breach notification, data transfers outside of the EU, and more

The report concludes with a discussion of the opportunities created by the GDPR. That's right—there are *business advantages* to complying.

THE CONTENT ADVISORY

The Basics:
Who and What Are Affected?

What is the GDPR?

The GDPR is a European Union law that regulates the use and disclosure of the personal data of anyone located within the 28 EU member states.[1] Violators face fines of up to €20 million or 4% of the firm's global gross revenue. (Regulators have stated that they will prefer the carrot to the stick. But it's also clear that they will not be pleased with firms that have not made an honest effort to comply.)

My company isn't located in the EU. Why should I care?

It is certainly correct that EU laws apply to the territory of the EU. So in the first instance, *companies* located within the EU must comply with the GDPR (even if the data processing takes place outside of the EU). However, the law also protects *people* located within the EU.[2] Thus any company, *regardless of location,* that processes the personal data of anyone located within the EU must comply with the GDPR if they either 1) offer goods or services in the EU (whether payment is required or not), 2) monitor the behavior of people within the EU, or 3) process personal data about people in the EU on behalf of an affected company (see Figure 1).

Key Terminology and Acronyms

Article 29 Working Party (aka Art 29 WP): An advisory body made up of a representative of each EU member state, the European Data Protection Supervisor, and the European Commission. The Art 29 WP regularly issues documents (aka opinions) that provide guidance on EU data protection law.

ePR: ePrivacy Regulation (see sidebar "The ePrivacy Regulation")

DPAs (aka supervisory authorities): Data Protection Authorities, or national authorities tasked with the protection of data and privacy, as well as the monitoring and enforcement of data protection regulations within the European Union.

Data controller: The entity that determines the purpose(s), conditions, and means of the processing of personal data.

Data processor: The entity that processes data on behalf of the data controller (does not include the controller's own employees).

Data subject: A natural person (as opposed to a legal person, e.g., a corporation) whose personal data is processed by a controller or processor. In a commercial relationship, this is usually the consumer, the term often used in this report. However, data subject rights apply equally to the personal data of other subjects, such as government constituents, donors to a charity, and employees.

ICO: The Information Commissioner's Office, the data protection authority for the UK.

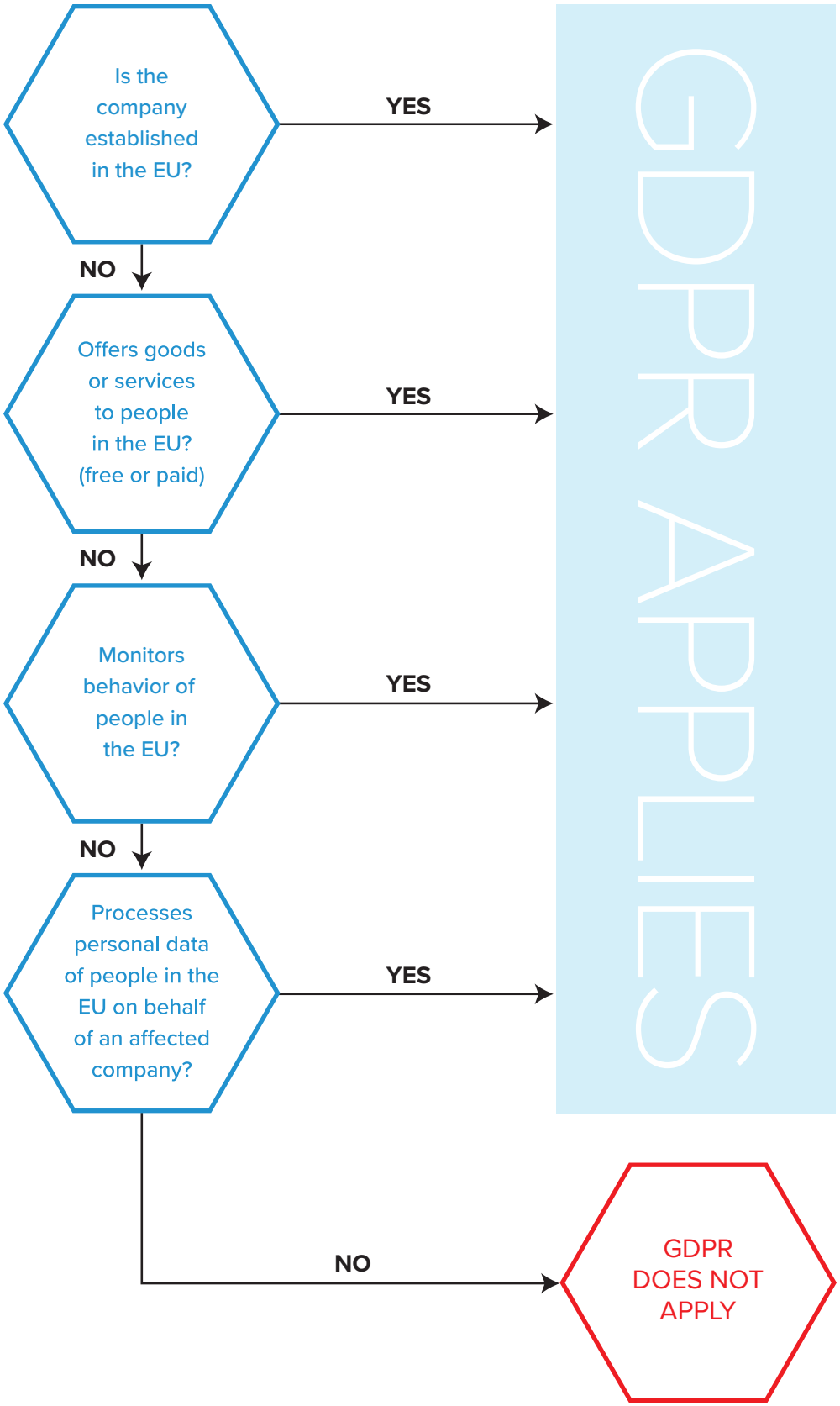
Personal data: Any information related to a natural person (i.e., data subject) that can be used to directly or indirectly identify the person.

Privacy by design: A principle that calls for the inclusion of data protection from the onset when designing systems (technical or otherwise), rather than as an addition or afterthought. The GDPR requires data controllers to practice data protection by design and to prove that they practice it.

Processing: Any operation performed on personal data, whether or not by automated means, including collection, use, storage, transmission, and so forth.

Source: Adapted from Eugdpr.org

FIGURE 1.


Is the company established in the EU?
YES
NO
Offers goods or services to people in the EU? (free or paid)
YES
NO
Monitors behavior of people in the EU?
YES
NO
Processes personal data of people in the EU on behalf of an affected company?
YES
NO
GDPR DOES NOT APPLY
GDPR APPLIES

Does the GDPR Apply to My Company?

We do business only in the U.S. Do we have to treat EU citizens differently because of the GDPR?

No, the GDPR has nothing to do with EU citizenship. Think of it this way: If the Austrian actor Christopher Waltz is browsing his Facebook profile while on the beach in L.A., he enjoys no more data protection than the US citizens surrounding him. Conversely, if Quentin Tarantino travels to Vienna to visit Waltz, they are both equally covered by the GDPR.[3]

What does "monitoring behavior" mean?

The GDPR specifically states that monitoring includes tracking people on the internet in order to create profiles and analyze or predict "his or her personal preferences, behaviors, and attitudes."[4]

Whoa – that sounds like a description of many common targeting and personalization strategies!

Indeed it does—and that is why marketers cannot just have the lawyers in the compliance department "take care of" the GDPR. The regulation will likely affect marketers and customer experience professionals more than many other roles, simply because of the many ways in which they use the personal data of customers and prospects.

Kind of crazy. It sounds like the regulators want to destroy any decent customer experience in the EU.

It's important to know that the GDPR is not the product of bureaucratic overreach by Brussels. The fact is that the EU Charter of Fundamental Rights includes the right to the protection of one's personal data. The European Parliament and regulators therefore have an *obligation* to formulate and enforce the GDPR, or something very similar. Also, there is a very sound argument to be made that putting people in control of their data will instill trust, increase the flow of data, and significantly improve the quality of customer experiences.[5] (For more details, see the concluding section of this report.)

Ok, you've got my attention. What counts as personal data?

Personal data is any information that allows you to identify a natural person (the data subject), whether directly or indirectly. That's a bit legal-esque, so let's break it down:

- A natural person is a living human being (dead people are not protected by the GDPR) and is in contrast to a legal person (e.g., a corporation).
- "Data subject" is the regulatory term of art for the person identified or identifiable via personal data. For the purposes of this report, we often refer simply to the consumer. But the GDPR applies equally to government bodies, nonprofit organizations, and the like. Also, employees enjoy virtually the same protections as consumers.
- Indirect identifiers are pieces of information that by themselves do not identify an individual but may do so when combined with other information. For example, using age, gender, or postal code alone is unlikely to help identify an individual. But when the three are combined they can uniquely identify nearly 90% of the U.S. population.[6]

Is personal data the same as personally identifiable information (PII) in the U.S.?

Since there are numerous federal, state, and local laws about data protection in the U.S., there is no single definition of PII. However, PII generally does not embrace indirect identifiers as broadly as the GDPR.

Can I get a complete list of everything that counts as personal data?

Not a chance. The regulators know that any such list would immediately be out of date. In fact, they try very hard to avoid strict, prescriptive rules, in an attempt to "future-proof" the GDPR.

What about digital identifiers?

The GDPR explicitly includes location data and online identifiers in its definition of personal data.[7]

So how about device IDs, analytics data, and cookies?

All are potentially personal data. The test is always whether *any* piece of information contributes to the identification of a natural person. However, the outcome of that test may depend on the context and circumstances. For example, the ICO (the data protection authority in the UK) has pointed out that "by itself the name John Smith may not always be personal data because there are many individuals with that name."[8] However, given a financial advisor with a small client base, even a very common name could identify a single person. Similarly, an indirect identifier such as a postal code may not be personal data if the company can show that it avoids collecting any information that could identify individuals when combined with the code.

What counts as processing?

Virtually anything you do with personal data counts as processing. The GDPR lists "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[9] But note that this series is introduced with "such as," so it is, again, not exhaustive.

What is this thing with data controllers and data processors?

A data controller is the entity that determines the purposes and the means of processing. A data processor is the entity that carries out the processing under the orders of the controller. Generally speaking, marketers will be acting as or on behalf of a data controller. (For more detail, see the Accountability section of this report.)

Consent:
Obtaining Permission to Use Personal Data

Is the consumer's explicit consent required in order to process their personal data?

FIGURE 2.

No. This is a very widespread misconception about the GDPR. First, consent is one of six legal grounds that can be used (if justified) for data processing. Others include servicing a contract, compliance with a legal obligation, and legitimate interest (see Figure 2). Marketing activities will very likely appeal to either consent or legitimate interest. Second, in most cases consent must be "unambiguous," which is a lower bar than explicit consent.[10]

What is the difference between unambiguous and explicit consent?

It can be illustrated as follows. Say that your office building manager informs you that on the first Monday of each month, a film team will shoot footage in the cafeteria; anyone present might be filmed. If, on the basis of this information, you enter the cafeteria at the designated time, you have given unambiguous consent to be filmed. However, you have not granted explicit consent, which would entail that you specifically acknowledge and state your agreement by, for example, signing a release form.

How can we be sure the consent we obtain meets GDPR requirements?

The GDPR requires that consent must be "freely given, specific, informed, and unambiguous." Each of these criteria is essential:

- **Freely given:** Consent may not be coerced or be the result of a power imbalance between the data controller and the data subject. For example, the data protection authorities discourage the use of consent in the workplace, on the assumption that employees may feel they cannot refuse an employer's request for personal data. In a commercial relationship, a company cannot make the provision of a service, such as internet search or a mobile app, dependent upon the collection of personal data, unless that data is *strictly necessary* for the service to function. (So that flashlight app that tracks your location and uploads your address book without clear consent would be illegal under the GDPR.)
- **Specific:** The consent request must clearly state what data is requested and what it will be used for. If there are multiple purposes, they must be stated separately.
- **Informed:** The consent request (and any associated content, such as a privacy notification) must be "presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[11] This is effectively the opposite of current practice, in which consent and privacy notifications are typically unilateral statements of the company's legal position, hidden in the terms and conditions and rarely, if ever, read carefully.
- **Unambiguous:** The GDPR states that unambiguous consent "should be given by a clear affirmative action."[12] "Silence, pre-ticked boxes, or inactivity" may not indicate consent.[13] If the consent request covers multiple processing purposes, they should be presented separately and enable a "granular" response (e.g., yes to "a" and "d" but no to "b" and "c").

What else goes into the consent request?

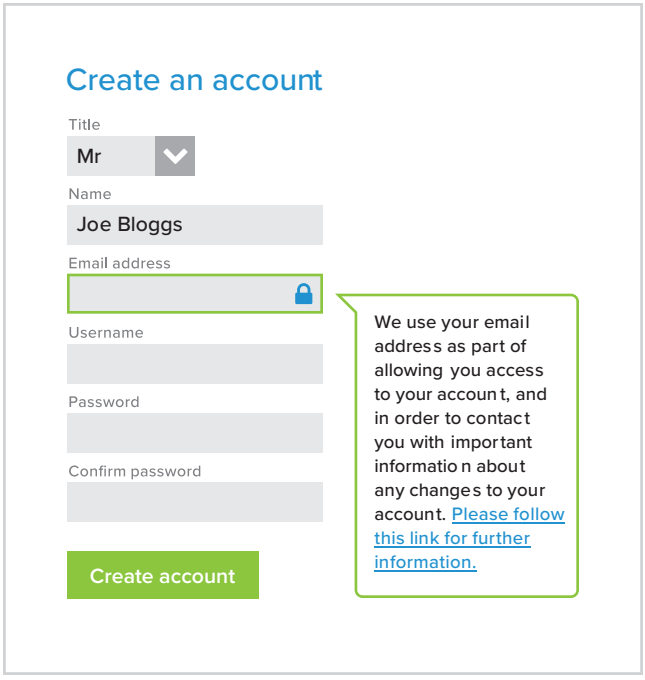
Lots. Article 13 of the GDPR spells out nearly a dozen categories of information that should be conveyed when data is collected, including with whom it will be shared, how long it will be stored, and whether it will be transferred outside of the European Economic Area, as well as the consumer's rights under the GDPR (see below) and the right to lodge a complaint with the data protection authorities.

Hold on—how are we supposed to present all of that in a concise and easily accessible way?

You're right, the requirements for transparency and fully informed consent are hard to reconcile, if not outright contradictory. The solution that has been endorsed by the regulators is so-called layered or just-in-time notification. For example, a data-capture form could reveal more information when the user scrolls over a given area (see Figure 3). The challenge—and the opportunity for competitive advantage—is to design these notifications in a way that both meets the GDPR requirements and provides a satisfying user experience. In fact, you might very well want to have multiple presentation formats that address the desires of various customer segments.

FIGURE 3. EXAMPLE OF A "LAYERED" CONSENT NOTIFICATION

Source: ICO.



Are there vendors that offer consent management solutions?

Yes. The International Association of Privacy Professionals' (IAPP) *2018 Privacy Tech Vendor Report* profiles more than two dozen consent managers.[14] Keep in mind that the challenge involves presenting, recording, storing, discovering, auditing, transferring, and potentially deleting the precise time, context, and consent of the consent request along with the consumer's granular response – as well as any subsequent revisions to or the repurposing of the collected data.

What counts as a specific, explicitly stated processing purpose?

The processing purpose is the cornerstone of data processing under the GDPR because it informs or determines what types of data are collected, how it is processed, how long it may be stored, whether processing is necessary and properly limited, and much more. Here again, however, the regulators are reluctant to issue prescriptive lists of acceptable purposes. However, they have clearly stated that "vague or general" (and very commonly used) purposes, such as "improving users' experiences" and "marketing purposes," will "usually not meet the criteria of being specific."[15]

Should we ask for consent for all of our planned processing purposes at once?

It depends. If you have established, trust-based relationships with some existing customers, you might feel confident that they will agree to a comprehensive data request, thus reducing your consent management workload. With prospects or new customers, however, it seems like a bad idea. A key to securing consent is to demonstrate the value that the consumer receives in return for their data (and ensuring that you deliver the promised benefit). That is hard to predict, or control, very far into the future. The approach should be to carefully map out the customer journey and ask for what you need when you need it. For example, ask an anonymous visitor for their email in order to send them a weekly newsletter or other useful content. If and when they become more engaged, ask for additional data to inform them of personalized offers, and so forth. In this way you avoid alarming consumers with a data request they might find intrusive at the beginning of the relationship, and you are better able to shape and deliver appropriate value propositions as the engagement develops.

Also, keep in mind that any personal data you request and use must be demonstrably *necessary* for a specific processing purpose. The core processing principles of the GDPR—such as purpose specification, data minimization, and storage limitation—mean that you may no longer collect

and aggregate personal data simply because "more is better" or because it might become useful in the future (see Figure 4).

Can we continue using the personal data we already hold?

Yes and no. No in the sense that there is no "grandfather clause" in the GDPR that exempts personal data collected prior to the regulation taking effect. But yes, you may continue processing existing data if—and only if—it was collected in a GDPR-compliant manner. The ICO's draft guidance on consent states that if existing consents "don't meet the GDPR's high standard or are poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing [. . .] or stop processing" the data.[16]

Should we contact people to ask for fresh consent?

If you want to continue using the data and an alternative legal ground is not available, then seeking re-consent (sometimes also called re-permissioning) may be the only choice. (However, see the discussion about existing customers in the Legitimate Interest section.) But be very careful! You need to be sure that everyone you are contacting for fresh consent has opted in to receive emails. Several companies in the UK have been fined when they sent appeals to update marketing preferences to people who had previously opted out of email marketing.[17]

My cherished contact database is beginning to look like a snake pit!

It certainly needs to be very carefully and thoroughly reviewed. The GDPR's "high standard" for consent encompasses both the requirements for consent

FIGURE 4. CORE DATA PROCESSING PRINCIPLES

Principle	Meaning
Transparency	Data Processing must be lawful, fair, and transparent (i.e., easily understandable).
Purpose specification and limitation	Personal data should be collected for a specific, explicitly stated purpose and not used for other, incompatible purposes.
Data minimization	The processed data should be limited to what is necessary to achieve the stated purpose.
Accuracy	Personal data should be kept accurate and up to date.
Storage limitation	Personal data should not be kept longer than is necessary to achieve the stated purpose.
Integrity and confidentiality	Data should be protected against loss, damage, and unauthorized processing.
Accountability	Crucially, companies ["data controllers"] must not only follow these principles, but also be able to document and demonstrate that they do so.

and the core processing principles. Just consider the email addresses you've collected. For each and every contact you currently hold, you need to ask, "Where did this come from?" "What (if any) purpose was given when we collected it?" "Was the purpose specific and explicitly stated?" "Is that purpose still valid?" "Has the storage period expired?" and much more. Take for example the common practice of collecting business cards or scanning badges at a conference "for a chance to win a new iPhone." According to the GDPR, the prize drawing is the stated purpose for processing (i.e., collecting) the personal data, and that is the *only* purpose for which it may be used. If you dumped those contacts into your master marketing database after the event, they are illegitimate (because the stated purpose has been completed) and should be deleted.[18]

To be clear, that doesn't mean that you can no longer collect contact information at a trade show! But if you intend to use the data for a prize drawing, for sending weekly newsletters, and for sales calls, those three purposes should be stated separately with an opportunity for the individual to grant or withhold consent for each.

Legitimate Interest: A Get-Out-of-Jail-Free Card for Marketers?

Consent seems pretty complicated. What about legitimate interest?

In the context of the GDPR, a legitimate interest is simply a benefit that accrues to a company or companies from the lawful processing of personal data. Recital 47 of the GDPR states that "The legitimate interest of a controller [. . .] may provide a legal basis for processing"—that is, it is one of the six legal grounds. It adds that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

Ah, an exemption for direct marketing!

Not so fast. First, note that Recital 47 says "*may be* regarded," not "*is to be* regarded." Some types of marketing may appeal to legitimate interest, but it is by no means a carte blanche exemption. Second, you don't simply *assert* a legitimate interest to justify processing. You need to conduct a so-called balance test that weighs your legitimate interest against "the interests or the fundamental rights and freedoms of the data subject" (the consumer).

How do we conduct such a balance test?

First, identify your legitimate interest. Examples provided by the regulators include "physical security" (e.g., of a power plant) and "conventional direct marketing and other forms of marketing and advertising."[19] Next, identify foreseeable impacts on consumers and any safeguards you could put in place to reduce or alleviate them. For example, you might send marketing messages to your existing customers but not allow your dealer network to have access to that email list. Third, carefully consider the "reasonable expectations" of the consumers and whether the exercise of your legitimate interest would amount to "unduly monitoring" them. This is the most important and also the hardest part of the test because, as the ICO notes, by relying on legitimate interest, "you are taking on extra responsibility for considering and protecting people's rights and interests."[20] (For this reason, you will want to work very closely with legal counsel when conducting a balance test.)

If the test weighs out in our favor, then we can process the data, right?

Yes, but you must first contact the affected consumers, explain your legitimate interest (and all of the other required information), and give them a *very clear* opportunity to object to the processing. In short, whereas consent involves an active opt-in, legitimate interest must present the chance to opt out. Also, processing under legitimate interest must still observe all of the core principles in Article 5 of the GDPR.

Give me an example of what kind of marketing is and is not allowed under legitimate interest.

The Article 29 Working Party has an unusually clear answer:

> Controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalize their offers and, ultimately, offer products and services that better meet the needs and desires of the customers.[21]

Great! That pretty much describes how we think of our profiling and personalization efforts!

I'll bet it does. But the passage continues:

> However, this does not mean that controllers would be able to rely on [legitimate interest] *to unduly monitor the on-line or off-line activities* of their customers, *combine vast amounts of data about them* from different sources that were initially collected in other contexts and for different purposes, and *create [. . .] complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent.* Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject (emphasis added).[22]

In short, legitimate interest "is most likely to be appropriate when you use people's data in ways they would reasonably expect and that have minimal privacy impact."[23] An example is contacting people who have purchased from you before to offer similar products and services or a relevant newsletter (in this sense, legitimate interest could help you secure your contact database with existing customers). However, the regulators have already excluded it as a justification for sophisticated, data-driven targeted marketing and advertising that relies on aggregating data to build profiles and predict behaviors or desires.

Data Subject Rights:
Putting Consumers in Control of Their Data

What about the rights granted to consumers by the GDPR?

In one of its early passages, the regulation states, "Natural persons should have control of their own personal data." The data subject rights (DSRs) are the most obvious way in which the GDPR achieves this aim (see Figure 5).

In effect, consumers may contact any controller to learn if and how their data is being processed and with whom it has been shared. They can demand an inventory of their data or a copy of it (delivered, the GDPR says, "in an easily machine-readable format"). They may insist that errors be corrected ("rectified") or that the data be deleted (the so-called right to erasure or the right to be forgotten). In certain contexts, consumers may object to further processing and claim exemptions from "automated processing" (e.g., where an algorithm makes decisions about credit worthiness). Finally, the GDPR contains a new right to data portability, meaning that a consumer may instruct a company to package their data, remove it from its own systems, and send it to another company.

FIGURE 5. DATA SUBJECT RIGHTS

Customers have the right to...	According to
...know how their data is being used, and by whom.	Article 13
...receive an inventory and/or copies of their data.	Article 15
...have inaccurate data corrected ["rectified"].	Article 16
...have their data erased [aka"right to be forgotten"].	Article 17
...restrict processing.	Article 18
...have their data sent to another provider ["data portability"].	Article 20
...object to data processing.	Article 21
...not be subject to automated processing and "profiling".	Article 22

How likely is it that consumers will exercise these rights?

In a survey of 1,000 adults in Ireland, 77% indicated they "plan to activate their new rights" under the GDPR. Over a quarter (26%)

indicated they would do so within a month after the GDPR takes effect.[24] According to a study of 7,000 people in seven EU states, 82% said they "plan to exercise their new rights to view, limit, or erase the information businesses collect about them."[25] However, whether people will make the effort to exercise the rights cannot be known with any certainty until they actually do so. For example, many of the DSRs are present in existing EU data protection legislation, but few companies have seen a flood of requests. On the other hand, crises such as the Equifax breach and the use of Facebook data by Cambridge Analytica may drive more consumers to take action.

How long do we have to respond to a request?

Under normal circumstances, one month.

How much can we charge for the effort required?

In most cases, companies may not charge for responding to a data subject request.

How can we be sure that a person is not requesting someone else's personal data?

Excellent question. Again, the GDPR places the burden on you as the data controller. In other words, it is not only a good idea to have a method to confirm the identity of the person requesting access to personal data; in order to prevent exposing data to unauthorized third parties, you have an *obligation* to do so. The GDPR does not prescribe precisely how this mandatory authentication procedure should be function. Recital 57 provides the example of verifying identity via the information "used by the data subject to log in to the online service offered by the data controller."[26]

We have personal data spread across dozens of systems—it's unrealistic to expect we can find it all.

The regulators are not likely to be sympathetic. The ICO has stated bluntly, "Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with" access requests.[27]

Certainly the burden of responding to the requests can be reduced significantly if your organization has conducted a thorough data inventory and created an actual or virtual aggregation layer, and if that layer pulls together data from various sources and provides a unified view of and access to the information you have from a given consumer.

Accountability:
Proving That You Are Compliant

Couldn't we just fly under the radar? How likely is it that a DPA is going to build a case against us?

The regulators don't need to have any evidence or suspicion that you are violating the GDPR. On the contrary, the burden is entirely on you. The accountability principle in Article 5 means that you not only have to comply with the regulation, you also have to be able to *prove* that you comply. The DPA just needs to knock on your door and ask to see your proof. (And the knock might come because the regulator has been tipped off by a consumer, an employee, or even a competitor.)

How do we prove that we're compliant?

Documentation. Perhaps the greatest day-to-day burden imposed by the GDPR will be the need to maintain extensive and detailed records. These must include all of your personal data processing activities, data protection impact assessments, consent requests and responses, legitimate interest balancing tests, contracts with and instructions to processing partners, responses to DSRs, data protection by design records, and more.

What is a data protection impact assessment?

A data protection impact assessment (DPIA) is a process to help you identify, understand, and alleviate or minimize the risk to data subjects posed by a proposed data processing activity. A DPIA is mandated by the GDPR in some instances and recommended in all others. The assessment may prove crucial in demonstrating to a regulator that you prepared properly for data processing and is a key part of data protection by design.

What is data protection by design?

Data protection by design (DPbD) is a framework that calls for proactively building data protection into technical systems and business practices from the outset, not as an afterthought or add-on.[28] In practice, this means that any business process that handles personal data (covering both the technical and human elements) must ensure that data protection has been embedded in *every step* of the design, creation, and operation of said process—from the first whiteboard session onward.

Does that change how we select vendors and service provider partners?

Yes, significantly. DPbD, and the GDPR more broadly, call for you to select and work with *only* those partners that are compliant and that can help you meet your obligations under the GDPR. Very carefully vetting all participants in a selection process is not just advisable; it is actually a requirement of data protection by design.

It sounds like a processing partner could expose us as a data controller to a violation.

That is correct. Unlike the previous EU legislation, the GDPR not only extends compliance responsibility to data processors, but it also makes data controllers and their processing partners jointly liable for violations. You need to make very sure that every link in the personal data processing chain is behaving properly.

What about third-party data that we purchase to supplement our data about consumers?

Similarly, as a data controller, you are responsible for the compliance of all of the personal data that you use, regardless of the source.

That could devastate the third-party data market.

Let's just say that you need to be careful, if not suspicious—or indeed paranoid—about the compliance of third-party data.

Other Considerations

Phew! And I thought the GDPR was mainly about data security.

Also a common misconception. In fact, just three of the ninety-nine articles in the GDPR address data security. Nevertheless, there are many important provisions that do not directly concern marketers and that we're not addressing here, such as the restrictions on the transfer of personal data outside of the EU (e.g., to the U.S.), the requirements for rapid notification after a data breach, and the need for many firms to appoint a data protection officer.

THE CONTENT ADVISORY

Opportunities for Marketers

The GDPR clearly requires a lot of work from the marketing team. What are the upsides?

I'm glad you asked. Here's a quick overview:

- **Cleaner databases:** The GDPR requires companies to know precisely what personal data they have and how to get a hold of it. Cleaning up and rationalizing data storage to be compliant will also solve the problem that marketers consistently identify as the primary barrier to improving customer experiences: siloed, fragmented, and redundant data sources.
- **Truly engaged customers and prospects:** As one observer noted, "When someone grants permission, they are acting consciously, becoming an active participant rather than a passive source of data to be pillaged. Permission equals engagement. And engagement is the ultimate goal here, isn't it?"[29]
- **Transparency:** The ignorance-is-bliss era, in which consumers blindly surrender personal data in exchange for internet services, is rapidly coming to an end. (Besides, it is basically outlawed by the GDPR.) When asked to name the number one reason they would abandon a merchant, 80% of consumers in a global survey said, "If they use my data without me

The ePrivacy Regulation

In conjunction with the GDPR, the EU has undertaken a revision of the current ePrivacy Directive. Like the GDPR, the new ePrivacy law will be issued as a regulation—binding on all EU member states—in order to provide a consistent standard of privacy across the European Union.

Whereas the GDPR is primarily concerned with the protection of personal data (for example, by ensuring that consumers remain in control of how their data is used), the ePrivacy Regulation (ePR) addresses the confidentiality of communications. For marketers, this covers mail, telemarketing, and email, as well as "over the top" messaging services such as SMS, WhatsApp, and Facebook Messenger. The ePR also regulates the placement of browser cookies (hence it is sometimes known as the "cookie law").

As of this writing, the proposed ePR has been accepted by the European Parliament Committee on Civil Liberties, Justice and Home Affairs and sent to the EU Parliament and the Council of Ministers, where the final text will be determined in so-called trilogue negotiations. It is not clear when the regulation will be implemented (sometime in 2019 or perhaps even 2020 seems likely) nor whether advertising industry and other business interests will be successful in loosening what they consider to be excessive restrictions on cookie use and consent for marketing communications.

The crucial question is, what happens when the GDPR takes effect on 25 May 2018, but the ePR is not yet finalized, let alone in force? The answer is that the GDPR applies to realms (e.g., electronic communications/marketing) currently covered by the ePrivacy Directive (and its member state implementations, such as the Privacy and Electronic Communications Regulations, or PECR, in the UK). ICO commissioner Elizabeth Denham was quoted in a recent article as stating, "Until the ePrivacy regulation comes into force, the current Privacy and Electronic Communications Regulations will sit alongside the GDPR, which means electronic marketing will require consent." This means, among other things, that the opt-out option for B2B email marketing allowed under the PECR is no longer available as of 25 May 2018.

knowing."[30] The transparency and rights mandated by the GDPR will give consumers what they clearly want: insight and control over how their data is used.

- **Delivering clear benefits to consumers in exchange for their data:** According to a Deloitte study, "62% of consumers are not confident that sharing their data with companies or public sector bodies will result in better services or more relevant products."[31] The GDPR requires marketers to request and use only the categories and volume of personal data that are *necessary* to achieve this processing purpose. This constraint will also empower marketers to explain with much more clarity and certainty what benefits consumers will receive as a result.
- **Building long-term relationships based on trust:** In a commercial relationship, trust is an *attitude* felt by consumers. Trustworthiness is a *property* of companies and brands. With the assistance of the GDPR, marketers can lead the effort to nurture consumer trust by *being* trustworthy, and to sustain it by demonstrating trustworthiness *consistently.*

For affected companies, compliance with the GDPR is not optional. But rather than an irritating regulatory burden, the GDPR can and should be embraced by marketers as an opportunity to clean up data repositories, communicate transparently with truly engaged consumers, and create long-term, trust-based relationships.

THE CONTENT ADVISORY

NOTES

1. The final text of the GDPR is available in English and 23 other languages at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-consil:ST_5419_2016_INIT. Throughout this report, references to the GDPR will be given by Recital or Article number and, where appropriate, paragraph number. Thus, Article 4(4) refers to Article 4, paragraph 4.
2. GDPR, Article 3.
3. See, "The Three Biggest Lies About the GDPR," https://www.linkedin.com/pulse/three-biggest-lies-gdpr-tim-walters-ph-d-/.
4. GDPR, Article 3(2)(b) and Recital 24.
5. See, "Can the GDPR Save CXM (From Itself)?" https://contentadvisory.net/can-gdpr-save-cxm/.
6. See, "Simple Demographics Often Identify People Uniquely," https://dataprivacylab.org/projects/identifiability/paper1.pdf.
7. GDPR, Article 4(1) and Recital 26.
8. See, "Determining What Is Personal Data," https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf.
9. GDPR, Article 4(2).
10. According to the GDPR, explicit consent is required when processing "special categories" of data that reveal, for example, "racial or ethnic origin, political opinions, religious or philosophical beliefs," and so forth. See Article 9. Explicit consent can also exempt a data controller from some restrictions, such as that on automated decision making. See Article 22.
11. GDPR, Article 7(2).
12. GDPR, Recital 32.
13. ibid.
14. The IAPP's 2018 Privacy Tech Vendor Report can be downloaded at https://iapp.org/resources/article/2018-privacy-tech-vendor-report/.
15. See the Article 29 Working Party's "Opinion 03/2013 on Purpose Limitation," http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Opinions such as this one that were issued prior to the GDPR and with reference to the previous EU Data Protection Directive (aka Directive 95) remain relevant since, as the Working Party has said in a recent opinion, "the GDPR codifies existing WP29 guidance."
16. See "Consultation: GDPR Consent Guidance" at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.
17. On the ICO's fines against Flybe and Honda, see https://www.theregister.co.uk/2017/03/28/ico_fines_flybe_honda/.
18. To be clear, a non-EU company participating in an event outside of the EU could continue the practice of collecting contact information for a marketing database. However, if the event was marketed in the EU, you would likely be required to filter out the collected information pertaining to residents of the EU, because their personal data is protected by the regulation when they return home.
19. Article 29 Data Protection Working Party, "Opinion 06/2014 On the Notion of the Legitimate Interest of the Data Controller," at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
20. See the ICO's guidance on legitimate interests, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.
21. See note 17: 25-26. Opinions such as this one that were issued prior to the GDPR and with reference to the previous EU Data Protection Directive (aka Directive 95) remain relevant, since, as the Working Party has said in a recent Opinion, "the GDPR codifies existing WP29 guidance."
22. ibid.
23. See note 18.
24. SAS commissioned a survey of 1,000 Irish adults in late May 2017. See https://www.sas.com/en_ie/news/press-releases/2017/august/irish-adults-intend-to-activate-new-personal-data-rights.html.
25. Pegasystems surveyed 7,000 consumers across seven EU countries. The report is available for download at https://www.pega.com/GDPR-survey.
26. The passages from Recital 57 reads, "Identification should include the digital identification of a data subject, for example through the authentication mechanism such as the same credentials, used by the data subject to log in to the online service offered by the data controller." The Article 29 Data Protection Working Party has offered additional guidance in this regard. See, "Guidelines on the Right to Data Portability," http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf: 11–12.
27. The ICO's Subject Access Code of Practice, https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf.
28. See GDPR, Article 25 and Recital 78.
29. "EU GDPR: When Rules and Regulations Offer Business a Golden Opportunity," https://medium.com/the-internet-of-me/the-eu-gdpr-when-rules-and-regulations-offer-businesses-a-golden-opportunity-b175174aee7c.
30. SAP surveyed 20,000 consumers in 20 countries for The Global 2017 SAP Hybris Consumer Insights Report, available for download at https://www.hybris.com/en/gmc55-the-global-2017-sap-hybris-consumer-insights-report.
31. See "Why the GDPR is Great for Marketers and Will Create a More Efficient Data Economy," https://econsultancy.com/blog/69399-why-gdpr-is-great-news-for-marketers-and-will-create-a-more-efficient-data-economy/.

The Content Advisory Inc.

We teach companies how to build audiences and see the future of strategic content through trend forecasting, research, education, and brand consulting.

A trusted audience is the most valuable asset any company will manage. For years, brands have had to rely on third-party media and measurement to reach the audiences who can drive strategic business value. We know that marketers now have the disruptive power to create or acquire owned-media experiences and build these valuable audiences for themselves. The Content Advisory is committed to accelerating this shift and fundamentally transforming the practice of marketing.

For more information please visit www.contentadvisory.net.