

How to Survive and Thrive Under the GDPR

An Essential Guide for Marketers

By: Tim Walters, Ph.D.



A DCG INSIGHT PAPER

HIGHLIGHTS

- 4 **Introducing the GDPR**
- 7 **Core Principles and Provisions That Matter to Marketing**
- 13 **Conclusion: Marketing in the Personal Data Economy**

Sponsored by

SIGNAL[®]



Executive Summary

Despite its name, the General Data Protection Regulation (GDPR) is not something that will be taken care of by the lawyers in the compliance department and the data security pros in IT. The GDPR – which takes effect May 25, 2018, and applies to every company that touches the personal data of people who live in the European Union (EU) – requires a company-wide and systematic response, ranging from senior executives and the board to HR, alliances, and front-line staff. In particular, however, the burden will be felt by those that have come to rely most heavily on the collection and processing of personal data – namely marketers and related customer engagement roles.

To be sure, the GDPR does pose significant challenges for data security and legal compliance, but these are largely extensions of existing practices (especially for EU-based companies).¹ For marketers, in contrast, the GDPR represents a genuine revolution, where freely collecting “data exhaust” is replaced by the need to get informed consent (or other forms of permission), and where the prevailing practice of acquiring the maximum possible amount of data is inverted into a regulatory requirement for “data minimization.”²

The data processing restrictions introduced by the GDPR will incent marketers to fundamentally rethink and redesign their strategies, processes, and day-to-day activities. But as it disrupts business as usual, the GDPR also creates the opportunity for marketers to build new and better interactions with consumers and to nurture relationships built on trust, active engagement, and mutual benefit.

In this report, we explore the most essential elements of the GDPR for marketers and show how and why the winners in the post-GDPR era will not be firms that merely *survive* by avoiding non-compliance, but rather those that *thrive* in the new environment by seizing the opportunities for richer, deeper engagement with prospects and customers. Beyond compliance – and armed with key tools such as a unified data layer – marketers will be on the front lines of the battle for precious consumer data.

Key Terminology and Acronyms

Adapted from eugdpr.org



Article 29 Working Party (Art 29 WP)

An advisory body made up of a representative from each EU member state, the European Data Protection Supervisor, and the European Commission. The Art 29 WP regularly issues documents (“Opinions”) that provide guidance on EU data protection law.

ePR

ePrivacy Regulation (see sidebar on p.6).

DPA

Data protection authority. National authorities tasked with protecting data and privacy as well as monitoring and enforcing the data protection regulations within the European Union.

Data controller

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

Data processor

The entity that processes data on behalf of the data controller. (Does not include the controller’s own employees.)

Data protection by design

A principle that calls for including data protection from the onset of designing systems (technical or otherwise), rather than as an addition or afterthought. The GDPR requires data controllers to practice data protection by design.

Data subject

A natural person whose personal data is processed by a controller or processor. In a commercial relationship, the consumer.

ICO

The Information Commissioner’s Office, the data protection authority for the UK.

Personal data

Any information related to a natural person (“data subject”) that can be used to directly or indirectly identify the person.

Processing

Any operation performed on personal data, whether or not by automated means, including collection, use, storage, transmission, etc.

Introducing the GDPR

From the North American perspective in particular, it's tempting to see a new EU regulation as just another layer of red tape dreamt up by some bureaucrats in Brussels. But the GDPR has deep roots in European history.

In particular, given the extreme surveillance, data collection, and subsequent prosecution of individuals both before and after World War II, it is unsurprising that *privacy and the protection of personal data* are embraced by some of the founding documents of the nascent EU in the 1950s, culminating in the Charter of Fundamental Rights of the European Union.³ In defense of these rights, the GDPR seeks to ensure that EU residents “should have control of their own personal data.”⁴

From a Directive to a Regulation: Data Protection for the Digital Age

The GDPR replaces the EU Data Protection Directive, better known as Directive 95. As the name indicates, this directive was adopted in 1995 – before the commercial World Wide Web, email, mobile devices, always-on connectivity, and the digitization and monetization of personal data on a massive scale. One of the primary motivations for the GDPR was the acknowledgement that digitization poses different and more numerous threats to the fundamental rights guaranteed by

the EU charter and that the directive required updating for the digital age. This means, for example, that “digital fingerprints” such as device IDs, IP addresses, and many browser cookie settings are explicitly counted as personal data under the GDPR.⁵

At the same time, however, the GDPR recognizes the business value of digitization and the processing of personal data, and aims to remove some of the barriers that have constrained companies operating across the EU. For example, Directive 95 required that each EU member state pass instituting legislation to achieve its aims. The predictable result was a hodgepodge of data protection requirements across the EU, creating a significant headache for international business. In contrast, a regulation such as the GDPR allows relatively little variation at the member-state level. In this sense, it serves the EU's goal to create a “digital single market” (DSM), relieving the burden on businesses that operate throughout the region.⁶ (Of course, there may be some disparity in how the member-state data protection authorities interpret and enforce the GDPR, but this is something they are aggressively working to avoid – precisely in light of the DSM.)

Also, unlike Directive 95, the GDPR is *extra-territorial*: it applies to any company that either offers goods and services to, or “monitors the behavior” of, EU residents – regardless of where the company is located or conducts its data-

The previous EU data protection guidelines were adopted in 1995 – before the commercial World Wide Web, email, mobile devices, always-on connectivity, and the digitization and monetization of personal data on a massive scale.

processing operations.⁷ This has the effect of “leveling the playing field” between EU- and non-EU-based companies when competing for business in Europe.

A Big Stick – But an Even Bigger Carrot

The remaining major difference between Directive 95 and the GDPR is the one that gets all of the attention – namely, the massive and, according to some, “life-threatening” monetary fines that may be imposed for non-compliance.

Under the national laws that were adopted to implement the directive, penalties varied widely. In the UK, for example, the current maximum fine is £500,000.⁸ In contrast, the GDPR states that fines should be “dissuasive” – that is, they should be painful enough to convince violators to permanently change their behavior. Specifically, maximum fines for a single violation can reach up to €20 million or 4% of a company’s *global gross revenue*, whichever is greater. For the largest companies, this could amount to fines of billions of euros.

But according to EU data protection regulators, the talk about massive fines and “crippling financial punishment” is mostly “fake news” and scaremongering.⁹ The UK’s chief data protection authority, Elizabeth Denham, has stated clearly, “The law is not about fines. It is about putting the consumer and citizens first.” Regulators, she adds, will continue to prefer “the carrot to the stick.”¹⁰

Seizing the GDPR carrot will not be simple; Denham allows that it may require “a change to the culture of an organization.” But “the benefit for organizations is not just compliance but also . . . an opportunity to develop the trust of consumers in a sustained way.”¹¹

Developing the trust of consumers – this is the vital task posed by the GDPR. Data may be the new oil, but the GDPR will make it impossible to extract and exploit this resource without establishing, nurturing, and sustaining consumer trust.

For marketers, the GDPR challenge is to use the regulatory *restrictions* as new possibilities for *relevance* and engagement and to see the core principles and provisions of the GDPR not as *barriers* to established practices but as *building blocks* for trust-based relationships that put consumers at the center.

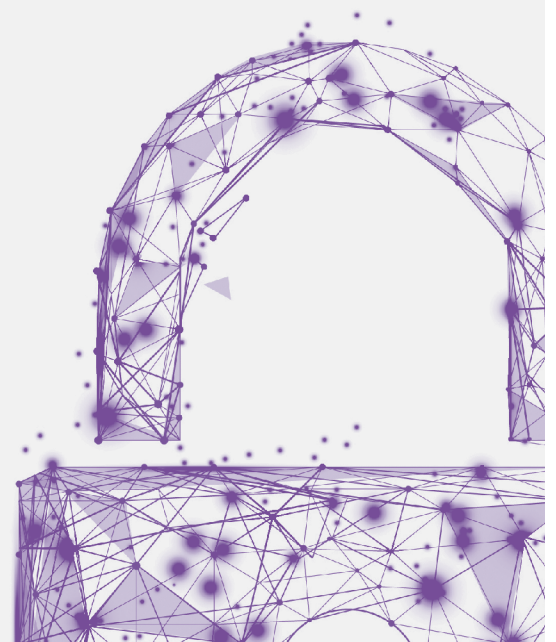
The UK’s chief data protection authority has stated clearly, “The law is not about fines. It is about putting the consumer and citizens first.” Regulators, she added, will continue to “prefer the carrot to the stick.”

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 Union.

Whereas the GDPR is primarily concerned with protecting 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 so-called “over the top” (OTT) 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 (late 2017), the proposed ePR has been accepted by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) and sent to the EU Parliament and the Council of Ministers, where the final text will be determined in negotiations among the three bodies. It is not clear when the regulation will be implemented (the original ambition to introduce it in line with the GDPR in May of 2018 now seems unlikely), 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.



Core Principles and Provisions That Matter to Marketing

The central philosophy of the GDPR is that personal data belongs to the person it identifies and that people should remain in control of their data.¹² As a result, companies that collect and process the personal data of EU residents are always only borrowing it for temporary use.

The commitment to maintain consumers' control over their data necessarily implies a set of *principles* that govern data processing activities (see Figure 1), and an associated set of consumer *rights* over the use of their data (so-called subject access rights, or SARs; see Figure 2).

The text of the GDPR effectively lays out the implications of these principles and rights for day-to-day business activities. For example, the accountability principle dictates that companies must keep careful records of all data processing activities, while the subject access rights mean that companies should respond to consumer requests about personal data within one month and at no cost, in most cases.¹³

For marketers, the most important provisions of the GDPR are covered in the following four sections.

Figure 1
Core Data Processing Principles (Article 5)

Principle	Meaning
Transparency	Data processing must be lawful, fair, and transparent (i.e., easily understandable)
Purpose 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 & Confidentiality	Data should be protected against loss, damage, and unauthorized processing
Accountability	Crucially, companies (“data controllers”) must not only follow these principles, they must be able to document and demonstrate that they do so

Figure 2
Data Subject Rights

Consumers 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

Consent: New Requirements for Data Collection

The GDPR provides six legal grounds for the processing of personal data; one of these must be designated for every processing activity. For marketers, the most important grounds are consent and legitimate interest.¹⁴

According to the latest available 2016 global survey by the Centre for Information Policy Leadership (CIPL), obtaining consent is by far the most popular basis for data processing, with over 90% of respondents using it to some extent.¹⁵ However, only about one-third of organizations were at that time able to meet the enhanced requirements for consent dictated by the GDPR.¹⁶ These include:

- Clear and concise consent requests
- A separate request for each processing activity
- An affirmative and “unambiguous” expression of consent that is “freely given”
- The ability to demonstrate the precise conditions and context of consent
- Comprehensive and detailed consent notifications

Asking for and receiving consent clearly serves the goal of putting consumers in control of how their data is used. The question, however, is how this philosophy will actually work in practice while

preserving the user experience. Without careful management it is easy to imagine that consumers will be plagued with endless consent requests and notifications, leading to what some have called “consent fatigue.”

For example: by definition, consent requests can be presented only by “first-party” sites or devices that have a direct interaction with the consumer. What, then, of the numerous third-party players that contribute to a customized digital experience with, say, analytic and personalization insights? One response, from the Interactive Advertising Bureau (IAB), is a proposed mechanism to obtain and distribute user consent among multiple participants in a customer experience ecosystem.¹⁷

Or again, consider the tension, if not contradiction, between the requirement for “clear and concise” consent requests and that for “comprehensive and detailed” notification, which should include the identity of the data controller, the processing purpose, the length of time the data will be held, third parties with whom it might be shared, whether it will be transferred outside of the EU, and much more. The proposed solution to this dilemma (endorsed by data protection authorities including the UK’s ICO) is a so-called “layered” or “just-in-time” consent request, with the key information provided concisely in the top layer and additional information in drill-down links or scroll-over pop-up windows.¹⁸

Without careful management it is easy to imagine that consumers will be plagued with endless consent requests and notifications, leading to what some have called “consent fatigue.”

Numerous vendors now offer “consent management solutions” to help companies meet the GDPR requirements. For example, Evidon’s solution exposes and tracks both first-party and third-party requests while avoiding information overload with layered notifications.¹⁹ (See Figure 3.)

What it means for marketers: When using consent as the legal ground under the GDPR, the consent request will be the key to the personal

data treasure chest – perhaps the *one shot* that the organization has to convince a consumer to provide the desired information. Instead of legal boilerplate, the consent request will be potentially the single most important communication between the company and the prospect. With this much on the line, marketers – the customer engagement experts – should be intimately involved with formulating, managing, and optimizing consent requests and notifications.

Figure 3.
Evidon’s Mock-up, With First-party and Third-party Consent Agreement

To learn about your privacy rights and our data practices, please see our [privacy policy](#). To learn more about our use of cookies and other tracking technologies, please see our [Cookie Consent Policy](#). To agree to our use of cookies, click "Accept" or to find out more, click "Options".

ACCEPT OPTIONS

WELCOME, OLIVER

SEEDS TOOLS CONTACT

Your Personal Data Rights

If you use any of Stewey's services, you a password and for restricting access to yo occur on your account. Stewey's does sell with a credit card or other permitted pay with the involvement of a parent or guar remove or edit content, or cancel orders.

Your Rights

Consistent with local legal requirements

- to access the personal data we hold
- to correct your personal data
- to restrict our use of your personal d
- to port your personal data
- to erase your personal data

You can make a request by using the form that we will likely require additional information

Type of Request*

Request access to personal data

Name*

Address*

Email*

Mobile Number Home N

Stewey's

Other Information We Collect About You

We want to be transparent about the data we and our partners collect and how we use it, so you can best exercise control over your personal data. For more information, please see our [Cookie Consent Policy](#).

Data We Collect

We use this data to improve our search results, show related content, sync promotional material, improve performance of our website, and send you emails about deals and savings on Steweys.com. You can opt-out of certain data uses by unticking the boxes below and clicking "Accept."

- Searches on steweys.com
- Recent purchases
- Cross-device tracking
- Browser History
- Email Marketing technology enabled

Data Our Partners Collect

Our partners use cookies to connect you to your social networks and collect information to better tailor advertising to your interests, both on this site and beyond. In some cases, these cookies involve the processing of your personal information. You can opt-out of the following third party cookies by unticking the boxes below and clicking "Accept."

- Facebook Advertising
- 4INFO
- DoubleClick
- Advertising.com opt-out through company
- Google Tag Manager this partner does not provide a cookie opt-out

ACCEPT

Privacy tools provided by EVIDON | [Learn more about your personal data rights](#)

Legitimate Interest: A Balance Test of Competing Interests

In the context of the GDPR, a legitimate interest is simply a benefit that accrues to a company from the lawful processing of personal data. The regulation states that “the legitimate interest of a controller . . . may provide a legal basis for processing . . .”²⁰ However, it continues, “. . . provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.”²¹

In other words, appealing to legitimate interest (LI) imposes an obligation on the controller to perform a rigorous “balancing test” that weighs the LI of the business against both the interests and the “rights and freedoms” of the consumer. Practical use of LI – and the extent to which it can shield current marketing practices under the GDPR – comes down entirely to the question of how this balancing test should be conducted and, for the business, what counts as tipping the scale in its favor.

Further clarification and guidance on such questions is expected from the EU data protection regulators near the beginning of 2018. However, existing EU guidance on legitimate interest states clearly that it *may not* be used to “unduly monitor” customers, to “combine vast amounts of data about them from different sources” or to “create complex profiles” of their “personalities and preferences” – precisely the sort of practices that drive many of today’s data-intensive marketing strategies.²²

What it means for marketers: It is entirely appropriate for organizations to consider

legitimate interest as the legal ground for some data processing activities. EU regulators have stressed that LI is not a “last resort” to be used only when consent is impractical or unfeasible.²³ Still, while additional guidance is pending, there is no evidence to suggest that the regulators will break with their previous opinions and now allow LI to justify practices they have so far held to be “intrusive” and “unreasonable.”²⁴ When legitimate interest is used, marketers should actively participate in – if not conduct – the balancing test, in order to provide crucial insights into the benefits that result for both the business and the consumer. Finally, note that data processing under legitimate interest still requires firms to, among other things, observe all of the principles and consumer rights, including data minimization and the ability to object to processing.

Dealing With Existing Data: No Grandfather Clause

The stricter requirements for data processing after the GDPR takes effect in late May 2018 raise an obvious question: What about all of our existing data? Is there a “grandfather clause” that allows previously collected data to be used under the new regulation?

Evidently, the answer is . . . yes and no. Yes, you may continue to use personal data that you currently hold – but *only* if it was acquired under conditions that meet the enhanced standards for consent dictated by the GDPR. The ICO acknowledges the burden this will place on many firms, but has so far refused to soften the restrictions on existing data:

“We appreciate that in some cases there may be a job to do in seeking new consent to comply with the GDPR standard. However, where existing consent falls short, this by definition is a necessary step in improving individuals’ trust, understanding and control over use of their data (assuming there is not a more appropriate lawful basis).”²⁵

As a result, most organizations should immediately initiate a thorough data inventory and audit with these goals in mind:

- **Discover and expose all existing personal data:** Merely *storing* personal data qualifies as “processing” under the GDPR, even if you’re not actively using it.²⁶ As a result, firms must expose the personal data that is held *anywhere and everywhere* in the organization – active systems, backups, employee PCs, thumb drives, etc. – as well as data that has been shared with partners or other third parties.
- **Determine the value of the business outcomes supported by the data:** With the advent of the GDPR, the risks associated with holding and using personal data increase significantly. The benefits derived from particular data sets must be weighed against these risks in order to determine whether they should be retained. (This data audit is also a great opportunity to clean house: Veritas Technologies estimates that 52% of all stored data is “dark” – collected and stored during normal business operations but otherwise unused – and another 33% is “ROT” – redundant, obsolete, or trivial.)²⁷

- **Understand the conditions and contexts in which the data was collected:** Does the data you wish to continue using require renewed, GDPR-compliant permissions? (In all likelihood, yes.)
- **Seek renewed consent from consumers:** Whenever possible, do so before the GDPR comes into effect and further complicates contacting consumers without prior permission.

What it means for marketers: An organization-wide data inventory certainly requires IT expertise. (Several vendors offer tools to help expose personal data in enterprise systems.) Still, only marketers can properly judge the value of a particular type of data to marketing outcomes and determine what legacy data the organization should seek to retain with re-consent campaigns. The request for renewed consent – essentially, “We have a bunch of your personal data and would like to keep using it” – unavoidably invites the consumer to reconsider the benefits of sharing her data and to potentially withhold permission. Small differences in wording, graphical design, and context could make a significant difference in the consent rate. Marketers should *formulate, test, and optimize* the requests for renewed consent for every desirable data set.

Data Portability: A New Battleground for Customer Data Allegiance

The GDPR introduces a new right to *data portability*. In short, this means that under certain conditions, a consumer may order that all of his personal data held by one data controller – say, a social network or a financial institution – should be bundled up and transmitted to a competing service or other data controller. Specifically, the right applies only to personal data that an individual “has provided to a controller,” and is restricted to data collected under the legal grounds of consent or performance of a contract. However, EU guidelines state that this extends to data “provided by” an individual by virtue of the use of a service or device – for example, purchase histories and browsing behaviors.²⁸

Portability is one of the most opaque provisions of the GDPR. As one commentator has noted, the general concept seems “purely theoretical,” since it “can’t be easily applied and doesn’t really correspond to any expressed or latent consumer’s needs.”²⁹

Still, EU regulators declare that portability is intended to avoid “lock-in” effects and switching barriers that could occur if consumers are unable to reproduce or transfer their data from one data controller to another. In this regard, the regulators hope to “support the free flow of data in the EU and foster competition between controllers.”³⁰ (They specifically describe how the ability to shift all of one’s existing data could help a new social network gain momentum.)³¹

In short, while responding to a portability request will likely be difficult and disruptive for most firms, the provision undeniably opens a new front for innovation and competition. Henceforth, firms can and should compete not only for customers, conversions, and “share of wallet” but equally for *the customer’s data* – which is potentially even more valuable than a conversion, due to the insights and enhanced offers that can be derived from it.

What it means for marketers: Data portability further empowers consumers, who can now offer sellers their data as well as their purchase power – and can “shop around” for the best offer from suppliers. It is likely that consumers will not be generous with their data – one recent study shows that 70% of surveyed adults over 55, 51% of those aged 35 to 54, and 27% of 18-to-34-year-olds currently provide consent less than 20% of the time.³² Marketers should strive to constantly craft and optimize campaigns and offers that go after competitors’ most valuable (e.g., data-rich) customers, while simultaneously strengthening the “data allegiance” of existing customers.

Conclusion:

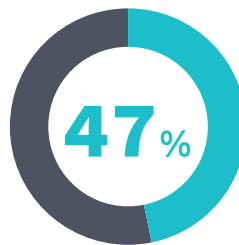
Marketing in the Personal Data Economy

The GDPR's avowed aim of putting consumers (back) in control of their personal data appears to resonate with consumers. As early as 2010, just one-quarter (26%) of social network users and less than one-fifth (18%) of online shoppers in the EU said they felt "in complete control" of their data online. Moreover, 70% said they feared their data was used for purposes beyond those stated when it was collected.³³

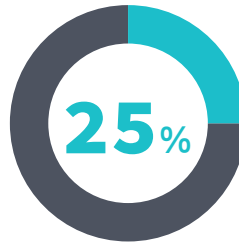
Most tellingly, Accenture's 2017 global survey revealed that consumers simultaneously crave more personalized services *and* express deep concerns about personal data privacy. For example, while 25% of those who abandoned a business did so due to poor personalization, 79% are frustrated that they feel they cannot trust companies with their personal information.³⁴ (See Figure 4.) Accenture concluded that this "significant digital trust deficit" must be addressed before firms can deliver the personalized and customized experiences that consumers seek and will reward.

In this context, the GDPR can be seen as a welcome impetus for organizations to ensure that their strategic use of personal data is understood and embraced by consumers. Despite the undeniable burdens it imposes, the GDPR's insistence on consent (or related forms of permission), transparency, and accountability manifestly puts consumers in control of the collection and use of personal data. *The regulation effectively*

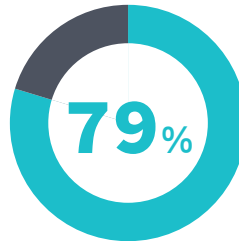
Figure 4
US Consumers Crave Personalization *and* Privacy



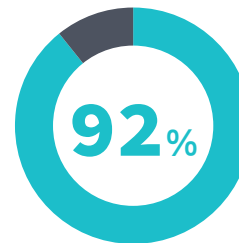
Expect specialized treatment for being a good consumer.



Who abandoned a business in past year did so because of poor personalization.



Find not being able to trust a company with personal information a top source of frustration.



Believe that companies should safeguard the privacy of their information.

Source: Accenture Strategy Global Consumer Pulse Research 2017. See Note 34.

Consumers will not be generous with their data. A recent survey shows that 70% of those over 55, 51% of those aged 35 to 54, and 27% of 18-to-34-year-olds currently provide consent for data collection less than 20% of the time.

makes customer-centricity a requirement for doing business in the EU. Rob Luke of the Information Commissioner's Office has said:

“Those organisations which thrive under GDPR will be those who recognise that the key feature of GDPR is to *put the individual at the heart* of data protection law. *Thinking first about how people want their data handled* and then using those principles to underpin how you go about preparing for GDPR means you won't go far wrong.”³⁵ (Emphasis added.)

Thriving – not merely surviving – after the GDPR means not only adapting to new restrictions but also acknowledging consumers' concerns, embracing the core principles of consumer control, and committing the organization to, as Elizabeth Denham says, “managing data sensitively and ethically.”³⁶


While the GDPR erects new hurdles to collecting and processing personal data, it is by no means hostile to data-driven marketing and wider business practices. On the contrary, marketers that get it right will have access to data from prospects and customers that have granted permission and have become active, engaged participants in the relationship.

After May 2018, the personal data of EU residents will become more scarce, but also immensely more valuable. Managing the available data will become even more critical, even as the task shifts from volume to quality and a single view of the engagement lifecycle. In a global survey by the World Federation of Advertisers, marketers named “connecting the dots between data stored across the organization” as one of the primary challenges presented by the GDPR.³⁷ A unified data layer will become virtually indispensable in order to respond to consumer rights such as data portability and the right to be forgotten, in order to improve security, and – above all – in order to understand and respond to consumers' desires and concerns about data sharing and usage. Come the GDPR, the commitment – and the ability – to manage data “sensitively and ethically” suddenly and unavoidably becomes the key to business success.

Notes

- 1 For a useful overview, see “GDPR: A Guide to Key Articles for Security and Privacy Professionals,” available at <https://www.forcepoint.com/resources/whitepapers/gdpr-guide-key-articles-security-privacy-professionals-hunton-williams>.
- 2 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. Here, Article 5(1)(c). Data minimization is one of the processing principles discussed below.
- 3 See for example the European Convention on Human Rights, drafted in 1950. Available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005>. The opening lines of the GDPR (Recital 1) immediately cite the right to protection of personal data from the Charter of Fundamental Rights: “Whereas, 1. The protection of natural persons in relation to the processing of personal data is a fundamental right.”
- 4 GDPR, Recital 7.
- 5 It is important to stress that the GDPR definition of personal data is considerably broader than that of most existing privacy legislation, including the notion of personal identifiable information (PII) as it is usually construed in the US. The unusual breadth in the GDPR arises from the regulators’ decision to include both direct and indirect identifiers. The latter consist of information that does not identify a person in isolation but can do so when combined with other information.
- 6 “Shaping the Digital Single Market,” at <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>.
- 7 The extra-territorial application of the directive was ambiguous and a matter of contention. “Previously, territorial applicability of the directive was ambiguous and referred to data process ‘in context of an establishment’. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear – it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.” Cited from <http://www.eugdpr.org/key-changes.html>.
- 8 “DPA Penalties and the ICO,” at <https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>.
- 9 See “GDPR: Sorting the Fact from the Fiction” on the Information Commissioner’s Office (ICO) blog at <https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/>.
- 10 Ibid.
- 11 See Elizabeth Denham’s January 17, 2017, speech, “GDPR and Accountability,” available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/>.
- 12 In the opening pages of the GDPR, Recital 7 states, “Natural persons should have control of their own personal data.” See also the January 17, 2017, speech by UK Information Commissioner Elizabeth Denham, in which she mentions control eight times, including, “People feel that keeping control of their most important information used to be simple, but that over the years, their sense of power over their personal data has slipped its moorings.” The speech is available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/>.
- 13 See GDPR, Article 12(3): “The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request.” For requirements regarding records of processing activities, see Article 30.
- 14 The six legal grounds outlined in Article 6 are: 1) consent of the data subject; 2) performance of a contract; 3) compliance with a legal obligation; 4) protection of the vital interests of the data subject; 5) performance of a task carried out in the public interest; 6) legitimate interest.

- 15 CIPL/AvePoint report, “Organisational Readiness for the European Union General Data Protection Regulation,” at https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/cipl_avepoint_gdpr_readiness_survey_report_1107_final-c.pdf.
- 16 GDPR, Article 7 and Recital 32.
- 17 Announced in late November 2017, the IAB initiative aims to enable “transmission of user consent choices to the supply chain, increasing accountability in the advertising ecosystem by enabling the creation of consent records and an audit trail.” The IAB has invited participation from other parties in the broad digital advertising and marketing ecosystem. See <https://www.iabeurope.eu/wp-content/uploads/2017/11/Press-release-IAB-europe-Industry-Consent-Mechanism-28112017.pdf>.
- 18 The ICO has issued a “Code of Practice on Privacy Notices, Transparency and Control.” Specifically about “layered” notices, the code states, for example, “There is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice.” See <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/where-should-you-deliver-privacy-information-to-individuals/>.
- 19 On Evidon’s “commercial grade” release, see <https://martechtoday.com/evidon-launches-first-commercial-grade-gdpr-solution-201524>.
- 20 GDPR, Recital 47. See also Article 6(1)(f). As often in the GDPR, the recital is indispensable for understanding the rather sparse coverage in the article.
- 21 Ibid.
- 22 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.
- 23 See the ICO’s September 2017 “Consultation on GDPR Consent Guidance,” a summary of the responses to the draft guidance on consent issued in March 2017. See <https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2172546/summary-of-responses-gdpr-consent-20171018.pdf>.
- 24 See note 22.
- 25 See note 23.
- 26 GDPR, Article 4(2): “Processing means any operation . . . which is performed on personal data . . . such as collection, recording, organisation, structuring, storage, adaptation or alteration . . . “ etc.
- 27 Gartner defines “dark data” as “information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes.” See <https://www.gartner.com/it-glossary/dark-data>. For the Veritas metrics, see <https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data>.
- 28 The right to portability is articulated in Article 20(1) of the GDPR. The Article 29 Working Party issued “Guidelines on the right to data portability” in December 2016. See http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf. The inclusion of browsing behavior is on page 9: “This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as “provided by” him or her even if the data are not actively or consciously transmitted.” The inclusion of purchase histories is on page 4-5.
- 29 See Pierre-Nicholas Schwab, “GDPR: what does data portability really mean?” available at <http://www.intotheminds.com/blog/en/gdpr-what-does-data-portability-really-mean/>.
- 30 Article 29 Data Protection Working Party “Guidelines on the right to data portability,” (revised April 2017) at http://ec.europa.eu/newsroom/document.cfm?doc_id=44099. (Automatic document download.)
- 31 Ibid.
- 32 “Why Age Matters When Gaining Marketing Consent,” at <https://www.consumerintelligence.com/articles/why-age-matters-when-marketing-consent>. See also “GDPR: Wake Up and Smell the Consent,” at <https://www.linkedin.com/pulse/gdpr-wake-up-smell-consent-david-cole/>.

- 
- 33 Special Eurobarometer report “Attitudes on Data Protection and Electronic Identity in the European Union,” at http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.
- 34 Accenture Strategy’s 2017 Global Consumer Pulse Research surveyed 25,000 consumers, including 2,000 consumers in the US, in June and July 2017. See <https://newsroom.accenture.com/news/us-consumers-turn-off-personal-data-tap-as-companies-struggle-to-deliver-the-experiences-they-crave-accenture-study-finds.htm>.
- 35 “ICO Issues Warning to Businesses As GDPR Countdown Reaches One Year to Go,” at <https://www.out-law.com/en/articles/2017/may/ico-issues-warning-to-businesses-as-gdpr-countdown-reaches-one-year-to-go>.
- 36 See Denham’s January 17, 2017, speech, “GDPR and Accountability.” Available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/>.
- 37 “Almost Three in Four Global Marketers Still Unaware of Full GDPR Implications,” at <https://www.marketingweek.com/2017/09/13/marketers-still-unaware-of-gdpr-implications/>. (Registration required.)

About Digital Clarity Group



Digital Clarity Group is a research-based advisory firm focused on the content, technologies, and practices that drive world-class customer experience. Global organizations depend on our insight, reports, and consulting services to help them turn digital disruption into digital advantage. As analysts, we cover the customer experience management (CEM) footprint – those organizational capabilities and competencies that impact the experience delivered to customers and prospects. In our view, the CEM footprint overlays content management, marketing automation, e-commerce, social media management, collaboration, customer relationship management, localization, and search. As consultants, we believe that education and advice leading to successful CEM is only possible by actively engaging with all participants in the CEM solutions ecosystem. In keeping with this philosophy, we work with enterprise adopters of CEM solutions, technology vendors that develop and market CEM systems and tools, and service providers who implement solutions, including systems integrators and digital agencies.

Contact Us

Email:

info@digitalclaritygroup.com

Twitter: [@just_clarity](https://twitter.com/just_clarity)

www.digitalclaritygroup.com