The GDPR Challenge

FOR CONTENT MANAGEMENT

By Tim Walters, Ph.D.

THE CONTENT ADVISORY

Sponsored by

Kentico

www.kentico.com

Executive Summary

Perhaps due to its name, the General Data Protection Regulation (GDPR) is often viewed as no more than a new data security law that will be taken care of by IT and the lawyers in the Compliance Department. On the contrary: the scope of the regulation and the manner in which it conflicts with accepted "best practices" in data-driven business operations mean that it poses an organization-wide challenge. Affected companies will have to review and potentially redesign **every single business process** that touches the personal data of EU residents in any way.

Nearly every business function will have new responsibilities and a role to play in ensuring compliance, from HR (for staff training) to the C-suite and the Board of Trustees (for strategic risk/benefit decisions). As one observer has noted, "The GDPR is not an IT responsibility, it is not a privacy [office] responsibility, it is not a marketing responsibility. It's rather a **company responsibility**."[1]

The challenges – and opportunities – are particularly numerous and complex for roles associated with content management and digital experience – developers, marketers, governance, analytics professionals, etc. Outside of the organization, it also impacts partners such as implementation firms, digital agencies, and cloud service providers. For many firms, the GDPR will complicate content creation, storage, sharing, publication, personalization, and optimization. At the same time, the regulation poses problems that can be addressed by a content management system (CMS), such as substantial new documentation requirements and the need to present, record, and track paired consent requests and responses.

In this report, we will first review the most important concepts and provisions of the GDPR, then address questions that it raises for the broad content management ecosystem, including vendors, system integrators, agencies, and associated software providers.

Getting to Know the GDPR

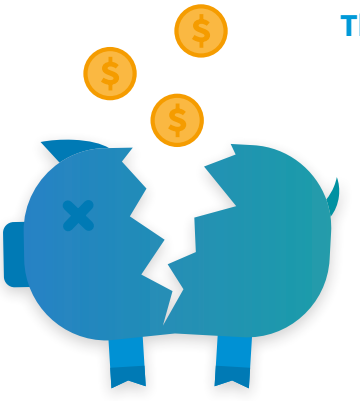
The GDPR was adopted in mid-2016 but included a two-year "transition period" before enforcement begins on May 25, 2018 – an indication that the EU regulators recognized how difficult it would be for many businesses to institute the measures for compliance. Nevertheless, few firms have taken advantage of the full grace period. One global survey at the beginning of 2017 found that over half (54%) of the responding organizations had not advanced their GDPR readiness.[2] Misconceptions about the meaning and full extent of the regulation are rampant. In a separate survey of multinational firms doing business in the EU, 31% said they felt they were already compliant. Yet, when asked about their ability to support specific provisions

"For many organizations, the GDPR will complicate content creation, storage, sharing, publication, personalization, and optimization."

of the GDPR – such as preventing unauthorized access by employees or confidently identifying and locating the personal data they hold – only 2% were judged to be ready. In addition, almost half believed – wrongly – that it is the sole responsibility of their cloud service providers to ensure compliance in the cloud.[3]

In light of such confusion, let's dive into the most important provisions and equirements of the GDPR.

A quick note on terminology: The GDPR distinguishes between **data controllers** – who dictate the purpose and the means of data processing – and **data processors**, who carry out the processing. We'll come back to this in the discussion of joint liability.



The Headline Grabbers: Massive Fines and "Extra-territorial" Reach

If you know anything about the GDPR, it's probably that violators face huge, potentially life-threatening fines. Indeed, the financial penalties can reach €20 million or 4% of a company's **global gross revenue** from the previous year. For example, that means BMW could theoretically face a fine of over €3 **billion**, based on 2016 global turnover. That compares to a current maximum fine (in Germany; it varies by EU member state) of about €300,000. That **10,000-fold increase** tells you that regulators have grown weary of companies (especially certain larger, US-based digital behemoths) that treat data protection penalties as a cost-of-doing-business. The GDPR specifically calls for fines to be "dissuasive" – that is, painful enough that they convince a company to fall into line.[4]

But the key word here is "theoretical": the fact that regulators **can** apply the maximum fines does not at all mean that they **will** do so in every instance – in fact, the regulation also calls for fines to be "proportionate".[5] Articles proclaiming that the GDPR will destroy small businesses in the EU ("23% of Irish organizations could be forced to close if found liable to fines"!) have been denounced by the UK's Information Commissioner, Elizabeth Denham, as "scaremongering" and "fake news".[6] She emphasizes that the data authorities "have always preferred the carrot to the stick".[7] Nevertheless, it's important to acknowledge that the large fines are available to the authorities when dealing with data-abusive "carnivores" that refuse to be satisfied with a diet of carrots.

Almost as famously, the GDPR has global reach. It is not geographically **restricted** to EU-based firms. Rather, it is geographically **defined** as regulating the processing of the personal data of any EU resident. (Not EU **citizens**. An Italian visiting the US is not protected.) Specifically, the GDPR applies to any organization (commercial or otherwise) that a) "offers goods or services" to EU residents, or b) "monitors" their behavior.[8] Critically for the broad content management ecosystem, this second point means that the GDPR applies to companies placing tracking cookies or selling analytics services without any direct relationship to the consumer (aka the "data subject").[9]

"The ICO commissioner stresses that authorities 'have always preferred the carrot to the stick.' Still, it's important to acknowledge that the large fines are available to authorities when dealing with data-abusive carnivores that refuse to be satisfied with a diet of carrots."

The Core Processing Principles and Data Subject Rights

It's tempting to view the GDPR (especially from a non–European perspective) as bureaucratic over–reaching that misunderstands how advertising fueled by personal data and tracking cookies is the indispensable monetization model of the "free Internet" and the broader digital economy.[10]

But in order to understand what motivates the data protection authorities (as well as the rather passionate independent privacy advocates in Europe), it's crucial to know that the GDPR has its origin in the EU Charter of Fundamental Rights, among which are counted privacy and the protection of personal data.[11] As the EU Data Protection Supervisor has bluntly stated: "There may well be a market for personal data, just as there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetize and subject a fundamental right to a simple commercial transaction."[12]

The right to protection of personal data has long be associated with an individual's ability to exercise control over the exposure and use of their data. The GDPR states "Natural persons should have control of their own personal data."[13] Ensuring such control necessarily implies that any processing of personal data must follow certain guidelines and restrictions. Thus, Article 5 specifies six processing **principles**:

1 **Lawfulness, fairness, and transparency**
Every processing activity must have a legal ground, be commensurate with other rights, and be communicated clearly.

2 **Purpose limitation**
Personal data should be collected and used for a specific, explicit purpose and not further used for other incompatible purposes.

3 **Data minimization**
The volume of data must be strictly limited to what is necessary to achieve the stated purpose.

4 **Accuracy**
Data must be correct and up to date (and deleted if accuracy cannot be ensured).

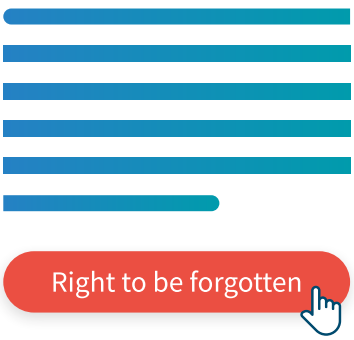
5 **Storage limitation**
Personal data must be stored no longer than necessary to achieve the stated purpose.

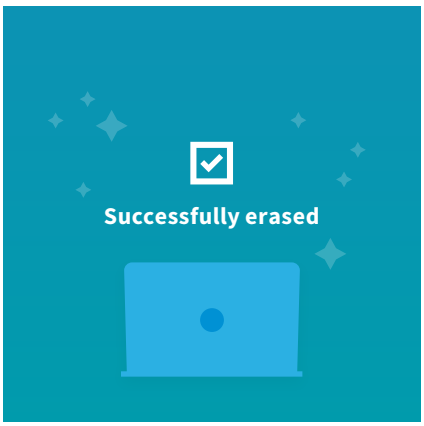
6 **Integrity and confidentiality**
Personal data must be protected from loss, damage, and unauthorized processing.

The second paragraph of Article 5 adds the principle of "accountability", namely, that data controllers "shall be responsible for, and able to demonstrate compliance with" the six principles. That simple sentence has profound implications. It means that organizations not only have to follow the principles and provisions of the GDPR, they also have to be able to **prove** that they do so. In effect, it means that you must follow the **spirit** of the law, not merely the letter. You cannot use grey areas or loopholes to escape from your "responsibility" to the GDPR.

The processing principles are complemented by the data subject rights that are spelled out in Articles 12–22. These state that a consumer ("data subject") has the right to:

- Know how their data is being used, and by whom (Articles 13 and 14)
- Receive an inventory of and/or copies of their data, in an "easily machine readable format" (Article 15)
- Have inaccurate data corrected (the right to "rectification" in Article 16)
- Have their data erased (the "right to erasure" or "right to be forgotten" in Article 17)
- Restrict processing of their data (Article 18)
- Have their data sent to another provider (the "right to data portability" in Article 20)
- Object to processing of their data (Article 21)
- Object to their data being subject to "automated decision-making" (Article 21)





Together, the processing principles and the data subject rights form the heart and soul of the GDPR. From them flow most or all of the obligations and restrictions that an organization must abide by in order to be compliant. For example, the much–discussed data security provisions – breach detection and notification, restrictions on international transfers, etc. – all express the principle obligations for data processing to be secure and protected from unauthorized use. Or again, the obligation in some instances to conduct a "data protection impact assessment" reflects the need to ensure that the proposed processing is lawful, fair, and does not unduly impact the "fundamental rights and freedoms" of the consumer.

The Key Content Management Workloads Created by the GDPR

This outline of the GDPR exposes the main workloads for content management processes and technologies.

He Said, She Said: Content and Notification Management

There are six legal bases for data processing under the GDPR.[14] Marketers and CX professionals will primarily use consent or so–called legitimate interest.

Consent is defined as "any freely given, specific, informed, and unambiguous indication of the data subject's wishes" to agree to personal data processing. Each one of these qualifiers is important:

- **Freely given:** The consumer must be reasonably able to refuse. Critically, this means that, in direct contrast to the prevailing funding model for most sites and apps, the provision of a service (such as Internet search, or a price comparison app) may not be made contingent on personal data processing – **unless** the processing is strictly **necessary** for the provision of the service

- **Specific:** Consent must be requested for a specific purpose; it may not be general or "omnibus". Separate consents are required for different processing purposes. (Or, bundled requests must present **granular choice**.)

- **Informed:** The consent requests must be in a "concise, transparent, intelligible and easily accessible form, using plain and clear language".[15]

- **Unambiguous:** Consent must be indicated by a **clear affirmative action**. Pre–checked boxes, designed opt–out, or implied consent by using a service are no longer valid.

In addition, consent must be as easily revoked as granted – implying that the option should be as prominently displayed, accessible, and understandable as the request. Finally, certain types of "sensitive data" require the higher level of explicit consent.[16]

Legitimate interest is a complex topic that cannot be explained in detail here.[17] To hear some marketing advocates tell it, however, the mere assertion of a legitimate interest magically excludes most of today's data–driven tracking, profiling, and personalization practices – a misconception that we'll explore below in the discussion of the GDPR's impact on targeted marketing.

For content management, the important point is that legitimate interest still requires the consumer's permission – in the form of a prominently displayed and intelligible opt–out option that must be presented to the consumer prior to any additional processing of the acquired data. Also, both consent and legitimate interest require that the consumer is fully and transparently informed about the purpose(s) and means of the proposed processing. The GDPR spells out a long list of information that must be conveyed in each case – including with whom the data will be shared, whether it will be transferred internationally, and how long it will be held. Thanks to the principle

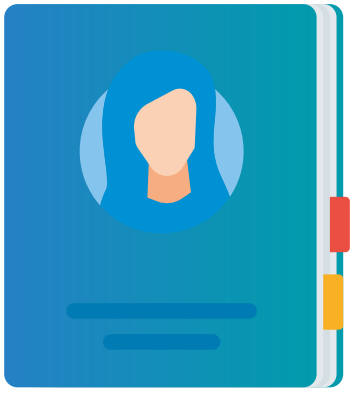
of accountability, it is, again, the data controller's responsibility to ensure – and to be able to prove – that the information was properly communicated, and then to be able to track, store, search, and recall the content and context of each communication as well as, in the case of consent, the consumer's yes or no response paired with every request.

A content management system is clearly well suited to this task. However, notification management is, or **should be**, about far more than tracking the presented content and the responses. Early studies show that consumers are overwhelmingly unwilling to provide consent when presented with a simple generic request. For example, one agency found that only 4% of consumers would share their spending habits with an airline when requested. But when the request offered a "personalized travel itinerary based on my budget", the positive responses shot up to 45%.[18] In short, **how** you ask for permission – the value proposition, the user experience, and the personalization of the entire interaction – will be crucial to securing access to the more rare and, therefore, more precious, personal data after the GDPR takes effect. Marketers can and should use their existing skills (and technologies) in customer research, persona building, targeting, and more in order to "market for permissions" and gain the data that they can use to fuel ever–richer user interactions as the customer engagement progress.[19]

Documenting Compliance: The Accountability Challenge

The need to document compliance is clearly the most burdensome workload imposed by the GDPR. Not only is it a new requirement in many respects, it is also ongoing and unrelenting – as opposed, say, to creating a system for notification management. In addition, the responsibility to prove accountability poses a kind of double jeopardy trap: An organization could be doing everything right for GDPR compliance, but, without proper documentation, still be found in violation.

"How you ask for permission – the value proposition, the user experience, and the personalization of the entire interaction – will be crucial to securing access to the more rare, and therefore more precious, personal data after the GDPR."



The GDPR requires meticulous documentation in areas such as:

- Records of all processing activities
- Justification of the selected legal ground for processing
- Consent requests and notifications (see above)
- How the "balance test" was conducted, if the legitimate interest ground is used[20]
- Data protection impact assessments (DPIAs, also known as privacy impact assessments, are required whenever the proposed processing may pose a "high risk" to the rights and freedoms of data subjects, and are recommended in other instances.)
- Data protection by design (see below)
- Prior and on-going communications with the relevant data protection authorities

A content management system with properly structured governance and workflows is practically indispensable for managing the documentation activities.

Where's My Data? Ensuring Data Subject Rights

If documentation is the most burdensome aspect of the GDPR, responding to data subject rights and so–called subject access requests (SARs) will be the most disruptive for most organizations. Responding to a single data subject request potentially involves being able to exhaustively identify **all** of that individual's relevant personal data; making an inventory report of it; copying it for delivery to the consumer; deleting it; and/or sending it to another controller (i.e., a competitor).

But to put it bluntly, the data and content infrastructures in use by most businesses simply do not support easily identifying, reporting on, and/or deleting all of an individual consumer's affected personal data. Data silos, redundant systems, and inflexible designs all contribute to the problem. For example, a resent GDPR eBook about the Salesforce marketing automation platform confesses that it is currently not able to support the "right to erasure" by fully deleting a record.[21] An IT manager at a large pharmaceutical company estimated that, due to the complexities of the current systems, responding to a single SAR would cost the company approximately €50,000.[22]

Nevertheless, many companies are likely to face a barrage of data subject requests soon after the GDPR takes effect. Among surveyed Irish consumers, 77% said they

intend to exercise their right to be forgotten.[23] Companies are expected to respond "without undue delay" and, in most cases, at no charge to the consumer.[24] Although the GDPR does grant some exceptions for SAR responses that would require "disproportionate effort", data authorities have said in the past that this does not excuse instances in which the information is simply difficult to access.[25] In fact, the ICO's 2017 SAR Code of Practice curtly reminds companies that "Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs."[26]

It is safe to say that the ICO has a facile attitude about facilitating SARs. The task potentially impacts nearly every aspect of the content management process, from product design to architecture, implementation, governance and metadata practices, and sharing content among partners and/or in the cloud. As the ICO added in the Code of Practice, "If you are buying a new information management system, you should consider including requirements in the specification about searching and SARs."[27]

"An IT manager at a large pharmaceutical company estimated that due to the complexities of the current systems, responding to a single subject access request would cost the company approximately €50,000."

Challenges and Opportunities for the Content Management Ecosystem

To reiterate, this report does not offer legal advice or guidance. However, we are now in a position to further explore some of the key questions the GDPR raises for the ecosystem of content management vendors, partners, agencies, and related software suppliers.

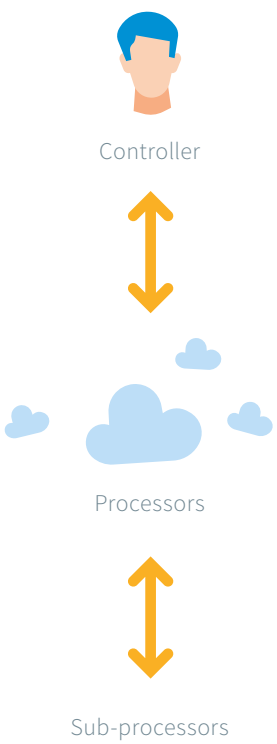
The Relationship Between Data Controllers and Data Processors

Recall the distinction between **data controllers**, firms that determine the purposes and means of personal data processing, and **data processors**, who carry out the processing on behalf of the controller (excluding the controllers own employees). It's the aspect of control that matters, not possession. A controller may never hold or store the data. And as soon as a processor uses personal data in any way that was not specified and directed by the controller (as the client), they become a controller (or joint controller) and will be treated as such under the GDPR.

A single controller undoubtedly employs many, perhaps hundreds of processors – a firm that stores archived data, an email campaign service, a social media analytics firm, or any cloud based software service, from Office 365 to a personalization platform. And each of these processors may use multiple sub–processors, and so on.

Under the previous Directive 95, data processors had no direct statutory obligations. Failure to conduct processing activities properly were a contractual matter between the processor and controller. The GDPR extends data protection compliance obligations to processors. Moreover, it makes the controller and its processor(s), as well as any sub–processors (called "other processors") mutually liable for violations (with some limitations noted below). This shift fundamentally transforms how the two parties must select, vet, and contract with each other.

Data Controllers and Data Processors



Data Subject

Controller

Processor

Key Questions

Can a single firm be both a controller and a processor?
Certainly. In fact, it is hard to imagine how any processor (say a social analytics firm) could operate their business without also using – i.e., controlling – the personal data of their customers, prospects, and employees.

What about firms outside of the EU that have clients in the EU?
What matters is not where the client is located but whether the personal data of EU residents is involved. If so, then the non–EU processor must abide by the relevant provisions of the GDPR. If a non–EU processor is not actively marketing to EU residents (say, they respond only to issued RFPs without active B2B sales efforts), they could **potentially** have little or no exposure to the GDPR as a data controller.

Are there any new roles that should be established?
The GDPR requires some firms (whether controllers or processors) – and encourages most others – to appoint a data protection officer (DPO).[28] This position requires an unusual mix of skills and expertise; still, by some estimates, over 75,000 DPO positions will be required worldwide by the GDPR.[29] Needless to say, the competition for highly–qualified candidates will be fierce. In addition, the GDPR requires many non–EU firms to appoint representatives in the EU.[30]

What is the effect on contracts and other agreements?
The effect is immense. Under the Directive 95, controllers were uniquely exposed to statutory requirements – but the maximum fines they could face were relatively low. (About €300,000 in Germany, for example.) In that context, controllers regularly could require processors to provide full indemnity, which processors were willing to provide in order to gain lucrative contracts. With controllers and processors mutually liable under the GDPR, and with maximum fines potentially reaching billions of euros, that habit will naturally end. Article 28 of the GDPR requires controllers to "use only processors providing sufficient guarantees to implement appropriate technical and organization measures" to comply with the regulation. This extreme vetting extends to every sub–processor as well; these may not be engaged by a processor without the authorization of the controller. As noted, processors must work strictly according to the directions of the controller. The contract between the controller and processor should restrict and bind the processor to the regulatory obligations of the controller – and this should flow down the chain of contracts with sub–processors, sub–sub–processors, etc. In short, because the GDPR provides no "grandfather clause" for existing contracts, virtually every controller–processor contract will have to be rewritten to ensure compliance by May 25, 2018.

Which party should take the lead in managing consent requests and other notifications to consumers?
In principle, the controller manages all communications around consent and other required notifications. Note, for example, that Articles 13 and 14, concerning the information that is to be provided to consumers, are addressed only to controllers. It is

conceivable that a controller could entirely outsource consent management and data collection to a processor, but then the latter must presumably work strictly on the instructions of the controller, which still determines the "purposes and the means" of the data processing.

Are there foreseeable mistakes in the controller/processor relationship that should be avoided?
Pre–GDPR, controllers and processors may have established an efficient "outcome based" working relationship, in which what matters is the end result of the processing of some collection of personal data, not the manner in which it is performed or even what third–party firms are involved. Given the strict requirements of the GDPR, such flexibility will likely have to end. Unless they want to risk being treated as controllers by the data authorities (and other parties that can bring complaints), processors must insist on working strictly to the instructions of their clients — and, again, rigorously document that they do so. Also, because of mutual liability, processors are going to have to be equally careful about vetting the controller's processes and safeguards around data collection, and potentially reject work from controllers who could expose them to risk.

A Special Note on Data Protection by Design

The GDPR obligates every data controller to practice "data protection by design". In short, 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.

Article 25 states that the data controller shall observe the principle of data protection by design "both at the time of the determination of the means for processing and at the time of the processing itself."[31] Recital 78 further clarifies that "producers of the products, services and applications" used in processing personal data — i.e., vendors and service providers — "**should be encouraged** to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, **to make sure** that controllers and processors are able to fulfil their data protection obligations" (emphasis added).[32]

We have seen that Article 28 restricts a controller to using **only** those processors that can ensure the controller's obligations under the GDPR. The requirement to practice data protection by design seems to extend this obligation to providers that would otherwise not count as processing partners – such as a vendor providing on–premise software or an agency that designs, but does not operate, a data–driven customer experience. When controllers shop for and select software and services from such

non–processor providers, they presumably will be negligent under the GDPR if they do not select solutions that enable them to "fulfil their data protection obligations." In other words, to be GDPR compliant, they must ask any and every vendor to demonstrate how the solution(s) facilitate data protection by design — and they cannot purchase a solution from a vendor who cannot provide a convincing answer.

The Impact on Targeted Marketing

After the GDPR, marketers and CX teams will almost certainly have access to significantly less personal data. The permission requirements – whether active consent or passively ignoring an opt–out – will reduce the amount of first party data. For similar reasons, the availability of third–party data will likely plunge dramatically. What consumer is going to provide consent to have their personal data aggregated and sold by a data broker to unknown clients and uses around the world? In fact, many observers predict "the death of third–party data" after the GDPR.[33] Finally, regardless of the quantity of available personal data, recall that one of the fundamental principles of the GDPR is "data minimization". In effect, controllers must be able to show that they have designed every process to use the smallest possible amount of data for the shortest possible period of time while exposing it to the smallest possible number of eyeballs and deleting it as quickly as possible when the processing purpose is complete.[34] Just ponder how that compares to current "max data" marketing practices and technologies!

Key Questions

Does the legitimate interest ground shield data–intensive marketing practices?

A lot of marketing gurus and industry groups would certainly like to have you think so. Appealing to Article 6(1)(f) on legitimate interest (LI), one so–called expert argued that the GDPR "is unlikely to have **any major ramifications** [for online marketing] in practical terms. This is primarily due to the revision of Art. 6, **the online marketing clause** of the GDPR" (emphasis added).[35] The author cites the associated Recital 47, which states that "the legitimate interest of a controller …may provide a legal basis for processing" and later adds "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

"Companies must be able to demonstrate that they have designed every process to use the smallest possible amount of data for the shortest possible period of time

while exposing it to the smallest possible number of people and deleting it as quickly as possible when the processing is complete."

However, this argument is deeply confused. First, there is no "online marketing clause" in the GDPR. Second, the reference to the legitimate interest of the controller as a legal basis is immediately followed by this proviso: "provided that the interest or the fundamental rights and freedoms of the data subject are not overriding." Every assertion of a company's legitimate interest, says Recital 47, "would need very careful assessment." Indeed, it requires that the company conduct a "balancing test" in which the purported legitimate interest of the company are weighed against the interest, rights and freedoms, and reasonable expectations of the consumer. Processing may be conducted on the legal basis of legitimate interest **only** when 1) this test is conducted appropriately (and it is hard to see how a company should be able to make a fair and objective judgement in this regard) **and** 2) the outcome is in favor of the firm's legitimate interests.

Even then, there are quite strict limits on what kinds of marketing activities are justified. The Article 29 Working Party's long and detailed opinion on legitimate interests (which, curiously, is never cited by the proponents of a **carte blanche** exemption for data–intensive marketing) grants that a pizza parlor that has collected a customer's name and address for a delivery has a legitimate interest in attempting to sell the customer more pizza, and may, therefore, use the personal data they hold to mail offers and discounts. But it adds that, in light of the customer's own interests, rights, freedoms, and expectations, legitimate interest **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 much of today's data–intensive marketing strategies.

How does the restriction on "profiling" and automated decision making impact marketing automation?

The provisions on profiling and automated decision making are among the most obscure in the text of the GDPR.[36] Fortunately, the Article 29 Working Party (WP) issued draft guidance on these topics in the Fall of 2017.[37] **Unfortunately**, the draft does not provide a clear judgement about the use of marketing automation.

The draft guidance defines profiling as a "procedure which may involve a series of statistical deductions… often used to make predictions about people." The WP emphasizes that merely sorting people into categories such as age and gender could be considered profiling. Automated decision making is defined as "the ability to make

decisions by technological means without human involvement." So far, that sounds like a functional description of much of today's algorithm–centric marketing stack.

However, the prohibition on profiling and automated decision making applies only when the resulting decisions have a "legal or similarly significant" effect on a data subject. In the GDPR, examples of such effects are "automatic refusal of an online credit application" and "e–recruiting practices without any human intervention."[38] On the one hand, the draft guidance states, "In many typical cases, targeted advertising does not have a significant effect on individuals…" But the "typical case" they provide is extremely simple: "for example, an advertisement …based on a simple demographic profile, 'women in the Brussels region.'"[39]

The WP goes on to say that it is "possible" for targeted advertising to have the "significant effect" that would trigger prohibition, and that the determination would depend on factors such as:

- The intrusiveness of the profiling process
- The expectations and wishes of the individuals concerned
- The way the advert is delivered
- The particular vulnerabilities of the data subjects targeted

In short, the draft guidance does not provide definitive clarity about the use of marketing automation tools. Reading between the lines, the Working Party seems to repeat the distinction that was evident in their 2014 opinion on legitimate interest cited above: straightforward advertising scenarios such as direct mailing to a previous customer (as in the pizza parlor example) or broad customer segmentations are acceptable. But aggregating large and varied data sets such as cross–device tracking and online/offline purchase histories for the purpose of creating complex profiles is problematic and probably requires consent. (This interpretation should be reviewed when the final guidance on profiling and automated decision making is released in 2018.)

How does consent change the relationship with a prospect?
Asking for permission to use personal data will reduce the amount of data available to marketers, perhaps substantially. But at the same time, it will vastly improve both the quality of the data and the relationship with the consumer. As one observer noted, "When someone grants permission, they are …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?"[40] In the GDPR era, the primary function of marketing will be to stimulate and nurture the permission that opens the treasure box of consumer data.

CONCLUSION

Embracing Customer-centrism

Excellent

Good

OK

Poor

Very Poor

Despite nearly a decade of effort, most companies still struggle to achieve success with customer experience management (CXM). For example, Forrester's CX Index found that 1% of 299 brands in North America deserved a rating of "Excellent". In France, no company ranked even "Good".[41] There are no doubt many factors that contribute to this failure: insufficient budgets, skill shortages, short–term thinking. Among them we must certainly count growing consumer resistance to the intrusive, surveillance–based marketing technologies and practices that are deployed by many companies. In a recent survey of adults in the US and the UK, over two–thirds (68%) said they don't trust how brands use their personal information.[42] Six out of ten consumers report they have falsified personal data they submitted online.[43] And when asked to name the number one reason they would abandon a merchant, 80% in a global survey said, "If they use my data without me knowing."[44]

The avowed goal of the GDPR is to curb marketing's insatiable appetite for data and put consumers back in control of how and when their personal data is collected, used, shared, and "monetized". One member of the EU Parliament has said that the regulators' aim is to "abolish surveillance–driven advertising".[45]

Content management has always been at the heart of CXM. Many of the players in the broad content management ecosystem will find the GDPR burdensome and costly. But if the transition is painful, it's worth remembering that the result will be – finally – genuine customer–centricity and real progress with customer experience management. We'll end with this remarkable comment from a member of the UK's Information Commissioner's Office (emphasis added):

"Those organizations which thrive under GDPR will be those who recognize 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."[46]

Notes

1. Scott Meyer, CEO of Evidon. See www.evidon.com/…/gdpr-un-readiness.

2. Vanson Bourne survey, at www.helpnetsecurity.com/…/gdpr-compliance.

3. The survey was conducted in February and March 2017 among 900 business decision makers in the US, the UK, France, Germany, Australia, Singapore, Japan, and the Republic of Korea. See www.veritas.com/…/…-they-are-gdpr-compliant.

4. 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 and, where appropriate, paragraph number. Thus, Article 4(4) refers to Article 4, paragraph 4. Here, Recital 151.

5. GDPR, Recital 151.

6. For the scaremongering Irish article, see https://businessandfinance.com/…/gdpr-fines-closure-irish-firms-datasolutions-survey/. Elizabeth Denham's reply is at https://iconewsblog.org.uk/…/gdpr-sorting-the-fact-from-the-fiction/.

7. Ibid.

8. GDPR, Article 3(2). The extra-territorial application of the previous data protection laws (based on the Directive 95) 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. GPDR 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 www.eugdpr.org/key-changes.html.

9. The GDPR and most other EU data protection documentation refers to the individuals identified by personal data as "data subjects." This reflects the fact that data protection legislation applies equally to individuals in their role as employees, governmental constituents, and consumers. In this paper, the focus is on commercial relationships; we therefore regularly refer to consumers rather than data subjects.

10. See for example a November 2017 article, "Euro-regulation Threatens Internet Model As We Know It," available at www.cityam.com/…/euro-regulation-…-know.

11. See the European Convention on Human Rights, drafted in 1950. Available at 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 fundament right."

12. See "Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, European Data Protection Supervisor, 14 March 2017" available at edps.europa.eu/…/…opinion_digital_content_en.pdf.

13. GDPR, Recital 7.

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. GDPR, Article 12(1).

16. Explicit consent is required when processing "special categories" of data that reveal for example "racial or ethnic origin, political opinions, religious or philosophical beliefs," etc. See Article 9.

17. Pending further guidance from the EU or member state-level regulators, the best insight on legitimate interest remains the Article 29 Data Protection Working Party, "Opinion 06/2014 On the Notion of the Legitimate Interest of the Data Controller," at ec.europa.eu/…/wp217_en.pdf.

18. The experiment was conducted by the digital agency Rapp UK. See www.thedrum.com/…/how-survive-the-data-apocalypse.

19. Numerous vendors are offering dedicated "consent management solutions" – which, of course, can be used to manage the communications and notifications when using other legal grounds besides consent. Vendors in this space include Evidon, PrivacyCheq, and Nymity. Platform vendors, such as Salesforce and IBM, are also building notification tracking capabilities into their solutions. The perceived need to "market for permissions" – thus to rapidly change the content, context, or UX of the notification – could give a content management solution an advantage over the limited templates and options of purpose-built solutions.

20. Appealing to legitimate interest imposes an obligation on the controller to perform – and document – a rigorous "balancing test" that weighs the LI of the business against both the interests and the "rights and freedoms" of the consumer. See also note 17.

21. The e-book was issued by salesforceben.com. It reports: "The inability to erase

people is something the Pardot team are working on." See www.salesforceben.com/gdpr-salesforce-ebook/.

22. Communicated in direct conversation, November 2016.

23. "The Irish Are Wising Up to Data Privacy, According to GDPR Survey," at www.siliconrepublic.com/enterprise/gdpr-ireland-data-privacy.

24. 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. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests."

25. See GDPR, Recital 62 and the review of the disproportionate effort "exemption" at www.lexology.com/…/detail.aspx?g=9ad8d210-355a-4c87-8bd8-2af4da32cd1f.

26. The ICO's Subject Access Code of Practice is available at ico.org.uk/…/subject-access-code-of-practice.pdf.

27. Ibid.

28. On the position and responsibilities of the DPO, see Articles 37-40. The Article 29 Working Party issued supplementary guidance in the spring of 2017. See www.twobirds.com/…/…-final-guidelines-on-data-protection-officers.

29. Based upon a study by the International Association of Privacy Professionals. See iapp.org/…/study-gdprs-global-reach-to-require-at-least-75000-…-worldwide/.

30. On the appointment of a representative, see Article 27 and Recital 80.

31. GDPR, Article 25.

32. GDPR, Recital 78.

33. For a somewhat more measured discussion of the impact of the GDPR on third-party data, see www.mycustomer.com/…/…the-third-party-data-market.

34. The principle of data minimization is stated in Article 5(1)(c). The desired behavior is expressed clearly in Article 25(2): The controller shall ensure "that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their

accessibility… to an indefinite number of natural persons."

35. "The New EU General Data Protection Regulation (GDPR): A Look At the New Regime From the Perspective of the Online Industry," at www.eprivacy.eu/…/…gdpr-a-look-at-the-new-regime-from-the-perspective/.

36. GDPR, Article 21-22.

37. The Article 29 Working Party draft guidance on profiling and automated decision making is available at ec.europa.eu/newsroom/document.cfm?doc_id=47742.

38. GDPR, Recital 71.

39. See page 11 of the draft guidance cited in note 34.

40. See Simon Carroll, "The EU GDPR: When Rules and Regulations Offer Businesses a Golden Opportunity," available at medium.com/the-internet-of-me/the-eu-gdpr-when-rules-and-regulations-offer-businesses-a-golden-opportunity-b175174aee7c.

41. The Forrester CX Index scale is excellent, good, OK, poor, very poor. See blogs.forrester.com/…/15-10-06-forresters_customer_experience_index_q3_2015_its_hard_being_an_optimist. and blogs.forrester.com/…/15-09-28-which_french_german_and_uk_brands_create_the_most_loyalty_with_their_customer_expe.

42. Gigya's 2017 State of Consumer Privacy and Trust survey is based on a survey of 4,002 adults, half from the US and half from the UK. See info.gigya.com/…/201704-Gigya-DS-Privacy_Survey_Report-web.pdf.

43. "Consumers Are 'Dirtying' Databases With False Details," at https://www.marketingweek.com/2015/07/08/consumers-are-dirtying-databases-with-false-details/.

44. SAP surveyed 20,000 consumers in 20 countries for "The Global 2017 SAP Hybris Consumer Insights Report." Available for download at www.hybris.com/en/gmc55-the-global-2017-sap-hybris-consumer-insights-report.

45. "Sippel: ePrivacy Reg Should 'Abolish Surveillance-Driven Advertising'," at iapp.org/…/sippel-eprivacy-reg-should-abolish-surveillance-driven-advertising/.

46. "ICO Issues Warning to Businesses As GDPR Countdown Reaches One Year to Go," at www.out-law.com/…/…gdpr-countdown-reaches-one-year-to-go.

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.