DIGITAL CLARITY GROUP

Insight Brief

Get Ready for the GDPR: Talking to Colleagues and Vendors

By: Tim Walters, Ph.D.

A Revolution in Digital Business?

It's been called "a revolution," "a paradigm change," and "a ticking time bomb."[1] Such language suggests that it's going to have a forceful impact and, for the unprepared, a potentially destructive outcome.

It bears the rather boring title of the General Data Protection Regulation, or GDPR.[2] But it's far from just another irritating policy cooked up by European Union (EU) bureaucrats. Instead, the GDPR is the most sweeping revision to European privacy and data protection legislation *ever*. It replaces a directive that was passed in 1995 – before the commercial World Wide Web, before email, before Google search, and before the digitization and monetization of personal data on a massive scale.[3]

Sponsored by

OPENTEXT™

And it isn't limited to the EU. The legal reach of the GDPR isn't defined by geography but by the use of the personal data of European residents. That means that it applies to *any* organization, located *anywhere* in the world that either "offers goods and services" to European residents or "monitors their behavior."[4] For affected firms, *every single business process* that touches personal data will have to be very carefully reviewed and, in all likelihood, redesigned to comply with the GDPR – or be scrapped.

That's just one of the disruptive tasks that the GDPR imposes on businesses before the regulation takes effect on May 25, 2018. Failure to meet the requirements will invite eye-watering fines of up to €20 million or 4% of the company's global turnover, whichever is greater. That's hundreds of millions or even billions of euros for large international organizations.

In short, the effort required to comply with the GDPR is immense – and the penalties for falling

short are even larger. It's obvious that 2017 must be the year for GDPR preparation. This report uncovers the key provisions of the regulation and provides a guide to kick-starting critical discussions, both internally and with vendors and service partners.

You Want Me to Do What? Key Provisions of the GDPR

The GDPR imposes substantially new requirements on numerous aspects of data collection and use, including the following:

- **What counts as personal data**. The GDPR defines personal data as anything that can be used to identify an individual either directly or when combined with other information. (By including indirect identifiers, the definition is broader than the concept of personally identifiable information [PII] used in many US jurisdictions.) The regulation specifically includes identifiers provided by digital devices and applications, such as IP addresses, browser cookies identifiers, and device IDs.[5]
- **Asking for consent to use data**. Many companies rely upon consent as the legal basis for collecting and processing personal data.[6] The GDPR requires that consent must be "freely given, specific, informed, and unambiguous."[7] "Specific" means that the consent request must state for what precise purpose the data is being collected; if more than one purpose is planned, the individual must be given "granular" choice – that is, the ability to consent to one purpose but not others. The requirement for "unambiguous" consent means that it cannot be inferred or assumed, or rely upon pre-checked boxes. Crucially, the provider of an online service (such as chat or web search) can require consent to collect personal data *only* if the data is required for the service.[8] Finally, any consent request must be "concise, transparent, and intelligible" – putting an end to dense legalese or hiding consent provisions in lengthy terms and conditions.
- **A careful balancing act for legitimate interest**. Aside from consent, businesses may appeal to their "legitimate interests" when processing personal data. For example, Recital 47 states, "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." This has encouraged some to argue that most digital marketing practices will be exempt from many of the restrictions enforced by the GDPR. However, firms are required to balance their legitimate interests against the "fundamental rights and freedoms" of the consumer. Direct marketing will likely be exempt only where the consumer is already

The GDPR applies to any firm, located anywhere in the world, that has anything to do with the personal data of European residents.

a client and has a "reasonable expectation" the firm would process data.[9] For example, the provider of a food delivery app may use the provided personal data (name, address) to mail follow-up offers. But they may not combine it with other data (from other apps, say, or location data from the phone) for the purpose of targeted marketing.[10]

- **New obligations for partners that process data**. The 1995 directive applied only to data controllers – that is, those that determine the purpose(s) for which data is processed. The GDPR extends responsibility for compliance to data processors – i.e., those who carry out the processing on behalf of a controller. For example, a payroll service provider is a processor, while its clients are controllers of the employee payroll data. The rapidly growing use of cloud-based services means that many companies will be served by a large number of data processor partners. Each of these relationships must be very carefully planned, monitored, and governed in order to ensure joint compliance with the GDPR.

- **The right to "erasure" and data portability**. The GDPR holds that individuals "should have control of their own personal data."[11] This extends to those times when the consumer has "loaned" her data to a business for processing. As a result, the GDPR allows any individual to contact any organization and request that their data should be: 1) rectified, i.e., corrected or updated if it contains errors; 2) erased, meaning that every piece of personal data about that person must be completely erased from all systems; 3) transferred to another firm (in an "easily machine readable format").[12] For example, I could direct Uber to bundle all of my personal data (name, credit card information, ride histories, location of frequent destinations, etc.), send it to Lyft, and erase all traces from its own databases. There are very few conditions under which a data controller is exempt from these requirements, and all requests must be complied with in a "reasonable" amount of time.

- **Accountability for the principles of data protection**. "Accountability" is the most fundamental and powerful obligation that the GDPR lays on affected firms. This dictates that it is not enough to follow the *letter* of the law. Instead, organizations must be able to demonstrate that, in their policies, processes, and behaviors, they embrace and embody the *core principles* concerning privacy and personal data protection that the GDPR advocates. Primary among these is the notion of data protection by design and by default. This requires that organizations design and implement both technical systems and business processes ("technical and organizational measures") that, from the outset and by default, are designed to minimize the exposure of personal data and respect the rights of so-called data subjects.[13] In practice, this means that firms must be able to show that every technical or business process that handles personal data has been carefully and conscientiously designed to use as *little* data as possible, for the *shortest* possible period of time, while exposing it to the *fewest* number of people, and deleting the data as *quickly* as possible when the processing is completed.

Warning: Don't count on the lawyers to deal with it alone

Obviously, the GDPR is not the kind of compliance issue that can be resolved by having legal counsel file a bunch of papers. Instituting and operating accountability for privacy and data protection as demanded by the regulation will require large-scale business transformation for most companies. Weighing the business benefits of personal data processing versus the risks will become a board-level issue.

Certainly legal, compliance, and IT professionals will play a major role in coming to terms with the GDPR. But so will marketing, vendor management, sales, customer service, HR, and many others. Data protection by design calls for a *systems thinking* approach, in which all parts of the organization work together as a systematic whole.[14]

Building Internal Awareness and Resolve – Engaging the Lines of Business

An effective response to the GDPR begins with building internal awareness of the challenges and opportunities it poses. Consider how this process should proceed from the affected lines of business (LOBs), including marketing or customer experience, sales, HR, and IT:

- **Get educated.** Papers like this one can provide a high-level overview. Afterwards, look for online resources, or bring in a consultant for an advisory.
- **Find out who has been assigned to investigate the impact of the GDPR**. In most organizations, this will be someone from compliance, legal, or IT.
- **Volunteer to help them understand how it will affect marketing**. By offering assistance, you can draw some organizational attention to your department, and lengthen the time available for an effective response.
- **Analyze the current use of personal data in your line of business**. For example, marketers know better than anyone how they use personal data. Map the data flows in web content personalization or email marketing, for example. If possible, find out what consents

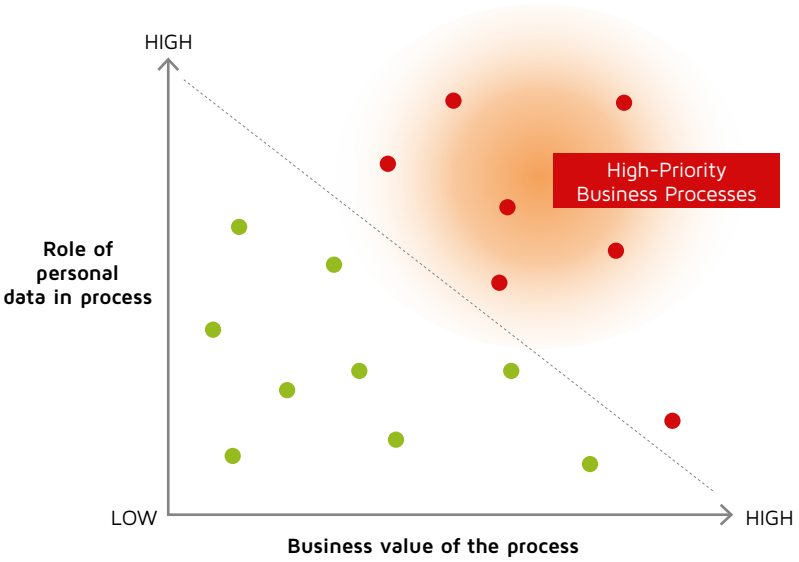
Companies must be able to demonstrate that any business process touching personal data uses as little data as possible, for the shortest possible period of time, and deletes it as quickly as possible – all while exposing it to the fewest number of people.

and stated purposes were attached to the data when collected. (The GDPR allows existing personal data to be used only if its collection was GDPR-compliant. Most likely, this will not be the case.) Moreover, look at the extent and amount of personal data in a given marketing process and the business value it produces. This allows you to identify and prioritize high-value, data-dependent processes for later comprehensive review and redesign (and will help secure the necessary funding and resources). (See Figure 1.)

- **Conduct a knowledge audit**. As awareness and momentum grow, network with other departments or teams and conduct a triage for organizational education about the GDPR. Who needs to know about the requirements (and opportunities) – from HR to the board of directors? How much do they need to know? (For example, an innovation manager we advised was justifiably most interested in how she could create new revenue streams by exploiting data portability.) How should we design an educational program so that each role receives the proper level of knowledge?

- **Participate in a data inventory and audit**. A thorough data inventory is an indispensable early step for GDPR compliance, but it's likely to be a lengthy and fairly technical project. Companies need to discover and analyze *all* the personal data they currently hold, *anywhere* – from core enterprise systems to backups, dormant databases, and thumb drives in employee backpacks. Studies show that the majority of data (especially unstructured data) held by a company is "dark" – that is, there's little or no indication that it even exists, or its business relevance is unanalyzed.[15] IT will do most of the heavy lifting during this discovery process (perhaps using emerging artificial-intelligence-based tools that help shed light on dark data), but marketing and other LOBs are uniquely able to judge the value of the data for business outcomes.

Figure 1
Identifying High-Priority Business Processes



Employees concerned about the GDPR should not remain silent. The compliance effort will be so disruptive that accelerating the corporate response in any way is a welcome contribution. Finally, don't be shy about playing the trump card: €20 million, or 4% of worldwide gross revenue. (And that's for a single violation!)

Vital Assistance: Finding the Right Vendors and Service Partners

GDPR compliance will substantially increase the importance of selecting the right technologies and forming deep partnerships with outside suppliers. In fact, the provisions for data protection by design effectively require that controllers and processors may work *only* with vendors and service providers with a demonstrated ability to help them meet their data protection obligations. In short, selecting or working with the wrong vendor could itself be a violation of the regulation.[16] At the earliest stages of a selection process, buyers need answers to questions such as these:

- **How do your products/services assist my data protection obligations?** Software vendors, or developers of customer solutions, should be willing and able to discuss security features such as access controls, secure information exchange, encryption, data leakage prevention, and breach detection.
- **Where do you store and/or process the data?** The GDPR tightens already strict limitations on the transfer of personal data outside of the European Union member states. As US-EU transfers appear likely to get only more problematic, vendors are increasingly investing in European data centers.[17]
- **How will your sales and service agreements reflect GDPR requirements?** With controllers and processors now jointly responsible for compliance (as noted above), buyers should favor providers that have taken the initiative to craft appropriate contract terms.
- **What is your roadmap for GDPR support?** Predictably, some "GDPR-washing" is already evident, with vendors suddenly branding their legacy solutions GDPR-compliant just because, for example, they are capable of storing and tracking some personal data. Look instead for providers with a thoughtful commitment to easing the compliance effort – and, beyond that, helping you innovate in the new environment.

After this initial vetting process, you can evaluate how the remaining providers help with the main GDPR workloads, including in these areas:

- **Data discovery and tracking**. In addition to the comprehensive data audit discussed above, data controllers need an ongoing ability to identify, track, and potentially remove the personal data of individual consumers, in order to respond to requests for rectification, erasure, or transfer to a different processor. In addition, data controllers must be able to reliably tag and track data with GDPR-mandated information such as for what purpose it was collected and when it should be deleted.

Predictably, some "GDPR-washing" is already evident, with vendors slapping "GDPR-compliant" on an existing solution just because it can store and track some personal data.

- **Business process analysis, design, and management.** Compliance will require near-constant monitoring of business processes to ensure that they meet the requirements for data minimization and purpose specificity. For example, how will you demonstrate that a given process uses the smallest amount of personal data possible and is handled by the fewest people possible?

- **Content management.** It almost seems out of place to talk about content management in the data-centric context of the GDPR. However, the regulation creates massive new content workloads, including creating and storing content requests and responses; detailed recordkeeping of data processing activities and outcomes; data breach notifications to individual consumers; and accountability requirements such as privacy impact assessments.

Choosing vendors and services providers has long been a special art that few companies perform really well.[18] Under the GDPR, neglecting the selection and vetting process could be literally illegal.

Conclusion

Look at it this way: The text of the GDPR is a gift from the future. It describes quite clearly how core aspects of the European business environment will change on May 25, 2018. Today's prevalent practice of "data maximization" – grab as much data as you can, and squeeze value out of it in any way possible – will be replaced by data minimization and purpose-limitation. Surveillance-based marketing will become effectively illegal; indeed, many aspects of today's digital advertising ecosystem will be rendered useless.

When the environment changes, the inhabitants must adapt . . . or die. Fortunately, for those companies that are willing and able, the GDPR can also serve as an instruction manual, spelling out what kinds of evolutionary adaptations are needed to not only survive but thrive under the new conditions. Compliance with the GDPR is the *requirement* in this new era. But ultimately, the *goal* should be to build and sustain competitive advantage in a business environment ruled by trust and respect for privacy. Quite frankly, that transformation around data collection and use – turning, in effect, from a wolf into a shepherd – will be impossible for some companies. Those that get it right can profit immensely from a whole new kind of customer loyalty.

Endnotes

1 These characterizations of the GDPR come from the following sources: Revolution: https://www.huntonprivacyblog.com/2016/10/05/cipl-gdpr-project-stakeholders-discuss-dpos-risk-gdpr/. Paradigm change: http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts. Ticking time bomb: http://commsbusiness.co.uk/news/gci-warns-gdpr-is-a-ticking-time-bomb/.

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.

3 The GDPR replaces Directive 95/46/EC, also known as the EU Data Protection Directive. As the title indicates, this Directive was adopted in 1995. Also note that as a directive, it required that each EU member state pass instituting legislation. The predictable result is a hodgepodge of data protection requirements across the EU, creating a significant headache for international business. The GDPR is, in contrast, a regulation and as such requires (with a few exceptions) no instituting legislation at the state level. In this sense, it serves the goal of creating a single digital market (SDM) across the EU, relieving the burden on businesses that operate throughout the region. Note that the GDPR consists of 99 articles, preceded by 173 recitals. The recitals have no legally binding force, but may be used to help interpret or understand a rule or requirement prescribed in an article. Throughout this report, articles are cited by number and, where appropriate, paragraph number. Thus, Article 4(4) refers to Article 4, paragraph 4.

4 "Monitoring" is generally equated with "profiling" in the GDPR. Article 4(4) defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." Arguably, this could describe any business that tracks and/or logs online behavior such as site visits using personal data such as IP addresses. More clearly, it applies to more intrusive activities such as tracking an individual across multiple sites, devices, or apps.

5 See GDPR, Recital 30: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." See also the definition of personal data in Article 4(1).

6 A 2016 survey by the Centre for Information Policy Law (CIPL) and Ave Point found that nearly half of responding firms rely on consent to process personal data. The survey further found that only about one-third of these firms are currently meeting the consent requirements of the GDPR. A summary of the findings, with a link to the full report, is available at https://www.huntonprivacyblog.com/2016/11/10/cipl-avepoint-release-global-gdpr-readiness-report/.

7 GDPR, Article 4(11).

8 For example, the collection of personal data may *improve* a web search engine, but it is not *necessary* for it to function. This would appear to mean that Google, for example, will have to give users the option of forbidding the collection of such data by May 2018.

9 GDPR, Recital 47.

10 The so-called Article 29 Working Party provides guidance on EU data protection legislation. (Under the GDPR, it will be replaced by a European Data Protection Board.) The Working Party issued guidance about legitimate interest in 2014, in the context of the Directive 95/46/EC; it seems very likely that most of this guidance will apply under the GDPR as well. The 2014 guidance states, for example, that controllers may not use 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 – and, for example, with the intermediary of data brokers, also trade in – 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." See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

11 GDPR, Recital 7.

12 See for example Recitals 65-67 and Articles 16-20. If a data controller has shared or made public the affected data, they must make "reasonable efforts" to ensure that any links or copies are also erased.

13 See Article 5 for an articulation of the core data protection principles, including purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

14 The Financial Times has defined systems thinking as "an approach that draws attention to connections among the parts [of a complex, dynamic system], particularly focusing on how the elements of a system feed back to one another." See http://lexicon.ft.com/Term?term=systems-thinking.

15 IDC has estimated that 90% of the data in a typical firm is "dark," meaning "data whose existence is either unknown to a firm, known but inaccessible, too costly to access or inaccessible because of compliance concerns." See https://www.linkedin.com/pulse/shedding-light-dark-data-bigdata-charles-fiori-cfa.

16 Recital 78 spells out the obligations of data controllers and processors: "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." It goes on to say that the "producers of the products, services, and applications" used in data processing (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.)

17 For a discussion of frameworks for data transfers between the EU and the US – namely, Safe Harbor and Privacy Shield – in the context of the GDPR, see http://www.digitalclaritygroup.com/gdpr-privacy-shield-sorting-out-business-obligations/.

18 Numerous resources for improving the software selection process are available at http://www.digitalclaritygroup.com/category/research/technology-selection-research/.

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

www.digitalclaritygroup.com