DIGITAL CLARITY GROUP

The Burden and the Benefit of Data Subject Rights Under the GDPR

By: Tim Walters, Ph.D.

A DCG INSIGHT BRIEF

To Appreciate Data Subject Rights, Look First at Customer Experience

One of the major areas of concern for organizations affected by the General Data Protection Regulation (GDPR) is ensuring they have the systems and processes in place to handle requests from individuals for information about, or access to, their personal data. Enabling the so-called data subject rights may be the first big challenge many organizations will face under the GDPR – as well as the first area both consumers and regulators will look at to check if an organization is in compliance.[1]

But to understand the importance – and potential value – of the data subject rights, it's best to begin by setting aside the text of the GDPR as well as any concerns about compliance and the specter of massive fines.[2] Instead, take a look at the current state of customer experience management (CXM). Global surveys of consumers – and who better to judge the state of customer experiences than consumers? – by the likes of Forrester Research and Accenture Strategy consistently show that most companies are making little progress in improving the quality of the experiences they offer.

Consider some of the evidence:

- In Forrester's September 2015 North American CX Index (CXi), 2.3% of the brands analyzed improved their rating over the previous study, while 28.5% got worse.[3]
- In Forrester's 2017 European CXi, a total of zero brands achieved an "excellent" rating.[4] In Germany, 83% were found to be "OK" (which for Forrester means mediocre), "poor," or "very poor."[5] In the UK, twice as many brands declined as increased compared to the 2016 ratings.
- On the 100-point scale for IBM's 2017 Customer Experience Index for the retail industry, the average score for all brands was a cringe-inducing 33 points.[6]

Sponsored by opentext™

The plight of CXM is often attributed to resource constraints; most companies don't have the required budgets, technologies, and skills to consistently offer exemplary experiences. But the results of Accenture Strategy's latest annual Global Consumer Pulse Survey point to an additional and more systemic issue.[7]

Accenture calls it a "vicious circle"; namely, consumers certainly favor and reward superior, highly personalized experiences, but the more they learn about how their data is collected, used, distributed, and sold – and potentially exposed to risk – the less they trust companies to "do the right thing." As a result, they are increasingly reluctant to provide the personal data that is the indispensable fuel for the very experiences they demand.

The virtue of consumer control over data

Accenture is far from being the only one to highlight the solution to this dilemma: placing consumers in control of how and where their data is used builds their trust and encourages them to provide more and richer data that informs ever more effective experiences. In short, shifting control to the consumer is the key to making real progress with CXM.

This is where the GDPR should come back into the calculation – for this kind of control is *precisely* the central goal of the regulation. (Recital 7: "Natural persons should have control of their own personal data.")[8] The data subject rights are the most direct expression of this objective. Instead of opaqueness and ignorance about how personal data is used and shared, the data subject rights seek to grant transparency, access, and control to the consumer. In this sense, while the GDPR and its support for data subject rights in particular may be a regulatory burden, they should also be embraced as an opportunity to provide precisely what consumers desire.

Terminology Used in This Report

Data Controller
The entity that determines the purpose(s), conditions, and means of processing personal data. In this report, often referred to as the company or organization. Note that the responsibility for complying with the data subject rights lies solely with the controller, not with data processing partners.

Data Processor
The entity that processes data on behalf of the data controller. (Excludes the controller's own employees.) Data processors have no obligations for the data subject rights, but must cooperate with and carry out the instructions of the data controller.

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

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.

Coming to Terms With the Data Subject Rights

The core data subject rights are presented in Articles 13-22 of the GDPR. (See Figure 1.) Basically, consumers have the right to know if a given company is using their data, how it is being used, and with whom it is being or has been shared. In addition, they can ask for a copy of the data, insist that errors are corrected ("rectified"), and, under certain circumstances, object to further processing. Finally, consumers may insist that their data is erased (the so-called right to be forgotten), require the company to package their data and send it to another company (the right to data portability), and claim exemptions from "automated processing" – e.g., where an algorithm makes decisions about creditworthiness.

Figure 1
GDPR 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

Many of these data subject rights are present in the existing EU data protection regulation (under the so-called Directive 95). Others, such as the right to be forgotten and the right to data portability, are expanded or new. Firms that have been operating in the EU under the existing rules should not assume that the impact of the GDPR will be minor, for enforcement has been lax and variable among the member states, and the fines have been manageable. (For example, in the UK, the maximum fine was 300,000 GBP.) The GDPR will introduce more consistent and aggressive enforcement practices, and maximum fines will be 20 million euros or 4% of the offenders' global gross turnover.[9] Efforts to support these rights immediately pose a number of practical questions, such as these:

- **What kinds of data are included?** The GDPR defines personal data as any information that can directly or indirectly identify an individual.[10] This now includes digital identifiers such as device IDs, IP addresses, location data, and many browser cookies. However, some data subject rights are restricted to certain types of data. For example, the right to data portability concerns

The key to sustained success in the experience economy is to grant consumers control over their personal data. That is precisely the aim of the GDPR and of the data subject rights in particular.

only data collected on the basis of the individual's consent or in order to service a contract.[11]

- **How can we confirm the identity of the individual submitting the request?** The regulation acknowledges that companies should confidently confirm the identity of consumers who request control over their data. Companies may request additional information and may eventually refuse the request if the identification is not sufficient.[12] However, since the practice of personalizing customer experiences is usually predicated on using unique identifiers such as email addresses, credit card numbers, or mobile device IDs, we can anticipate that the data protection authorities (DPAs) will expect companies to rely on similar means to confirm the identity of data subject requests.
- **How long do we have to respond?** Companies should respond to requests within one month; if not, the consumer may complain to the relevant data protection authority. If a company receives a very large number of requests and/or very complex requests, the response may be extended by an additional two months.[13]
- **How much may we charge?** In most cases, companies may not charge for responding to such requests. The GDPR does allow the application of a "reasonable fee" in the case of "repetitive requests" or requests for additional copies of the personal data held by the company.[14]

Will Consumers Exercise These Rights?

It's been called the million euro question: To what extent will the EU residents covered by the GDPR exercise their data subject rights?[15] Predicting the volume of requests seems absolutely crucial in order to determine the investments that companies should make to appropriately respond to them.

The available evidence suggests that companies should prepare for the worst:

- **SAS surveyed 1,000 adults in Ireland:** 77% indicated they "plan to activate their new rights" under the GDPR. Over a quarter (26%) indicated they would do so within a month after the GDPR takes effect.[16]
- **Pegasystems surveyed 7,000 people in seven EU states:** 82% said they "plan to exercise their new rights to view, limit, or erase the information businesses collect about them."[17]

It is appropriate to be suspicious of these early surveys. First, it's not entirely clear how the questions were worded; SAS, for example, evidently asked the Irish participants whether they "would welcome the opportunity" to access their data. Also, Pega points out that nearly 80% of the respondents were initially unaware of the GDPR. It was only after the data rights were explained to them that a similar number expressed a desire to take advantage of them. Even then, the results varied from 90% in Italy to 74% in the UK. In short, predicting the volume of requests your company will receive is quite speculative.

But any uncertainty about the volume of subject access requests may be outweighed by the GDPR's accountability principle, which states that data controllers "shall be responsible for *and able to demonstrate compliance with*" the requirements of the GDPR [emphasis added].[18] In other words, affected companies not only have to comply with the GDPR, they also are expected to be able to *prove* that they comply. This implies that if a DPA initiated an audit (and they can do so at any time, even in the absence of a consumer complaint), the DPA could expect an organization to demonstrate a reliable capability to respond to data subject requests *regardless of the volume of requests actually received*.

What if the technologies don't cooperate?

Many companies may find that their sincere commitment to supporting the data subject rights is thwarted by the technologies and processes they use for processing personal data. For example, CRM and marketing automation systems are frequently designed in a way that makes it practically impossible to "forget" data. (Deleting a record might only place it in a "recycling bin" so it can be reactivated if the individual re-engages with the company.)[19] Moreover, the data subject rights require the data controller to make a reasonable effort to inform any other organization with which the data has been shared, such as processing partners. But again, many systems and supporting processes do not reliably record and track the distribution of data with third parties.

In this regard, the data protection authorities could conceivably grant some leeway where the data subject right is new and technically unproved – e.g., the right to data portability. But for those rights that have long been established prior to the GDPR, such as the right to access information about what data is held, and how it is shared and processed (the so-called subject access request, or SAR) the authorities are unlikely to be sympathetic to the burden imposed by existing technology and processes. Indeed, the Information Commissioner's Office (ICO), the UK's DPA, has stated bluntly, "Given that subject access has been a feature of data protection law since the 1980s, your information management systems should facilitate dealing with SARs."[20]

Preparing to Support the Data Subject Rights

The ICO has also warned that responding to data subject requests – which again means granting consumers control over their data – will be impossible "without adequate information management systems and procedures."[21]

When Pegasystems surveyed 7,000 people in seven EU countries, 82% said they plan to exercise their new rights to view, limit, or erase information.

Preparing to support the data subject rights (and comply with broader GDPR requirements) entails three main steps:

- **Clean house:** "Do you have any of my personal data?" Responding accurately and confidently to this simple question requires an organization to have uncovered and understood *every single piece* of (potential) personal data throughout the enterprise – and beyond, for it includes data that has been shared or transferred. The first step to GDPR compliance is thus a *comprehensive* data inventory. Then comes an equally comprehensive audit and analysis: Is this asset personal data? Where did it come from? What rights (such as user consent) are attached to it? Where is it stored? How and why do we process it? What business value does it create? Do we want to continue to process it? If so, what permissions should we secure? At this point you are in a position to confidently delete unnecessary or unwanted data, retire legacy systems, etc. More importantly, you can better explain to consumers the benefits *they* will derive by allowing you to use their data.
- **Set the table:** Remember, you have one month to respond to what could be a flood of data subject requests, and in most cases you must do so at no charge. To contain the cost of compliance, you need to ensure that responsible staff can quickly locate, access, rectify, copy, and/or delete all of the relevant personal data for an individual consumer. This could entail rationalizing and unifying repositories, optimizing metadata and tagging practices, and providing dashboard tools for data discovery and analysis.
- **Secure the right ingredients:** With the clutter cleared away and a plan in place for receiving the guests (i.e., requests), you should confirm that you have the appropriate tools and skills on hand. Technologies likely to play a role in supporting the data subject rights include enterprise content management (ECM), records management (RM), permission and access rights management, archiving solutions, and tools for data discovery, analysis, and visualization.

In effect, the GDPR's legal requirements are also a welcome opportunity for affected organizations to review, rationalize, and improve their content and data management infrastructure and business processes.

Conclusion

From a narrow regulatory perspective, the GDPR will be seen as an unwelcome and perhaps unnecessary burden. Affected companies have no choice but to implement the systems and processes that place and maintain consumers in control of their personal data. But from the broader and far more important perspective of businesses competing on the basis of the experiences they offer to increasingly demanding and fickle consumers, the GDPR should be embraced as a fortuitous and powerful incentive to make the changes in the collection, processing, and governance of personal data that consumers – not regulators – demand. Satisfying the requirements for data subject rights under the GDPR is also a giant step towards breaking out of the "vicious circle" – namely, by granting a sense of control, which will build trust, which will encourage consumers to provide the data that companies need to build the experiences they crave and will reward with their business and loyalty.

For affected firms, the GDPR and the data subject rights in particular are inescapable. But for all firms, they are also arguably the best, if not the only, way to compete successfully in the data-driven experience economy.

Notes

1 The member state data protection authorities (DPAs) will likely be swamped with work after the GDPR takes effect on May 25, 2018. But this should not encourage affected firms to "play the odds" hoping to escape detection, for both individual consumers and independent privacy advocates can bring cases to the attention of a DPA and trigger an investigation.

2 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." She emphasizes that the data authorities "have always preferred the carrot to the stick." 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. For the scaremongering Irish article, see https://businessandfinance.com/news/gdpr-fines-closure-irish-firms-datasolutions-survey/. Elizabeth Denham's reply is at https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/.

3 "Forrester's Customer Experience Index, Q3 2015: It's Hard Being an Optimist," at http://blogs.forrester.com/michael_gazala/15-10-06-forresters_customer_experience_index_q3_2015_its_hard_being_an_optimist.

4 "Forrester Releases France, UK & Germany 2017 Customer Experience Index Results," at http://www.prnewswire.co.uk/news-releases/forrester-releases-france-uk--germany-2017-customer-experience-index-results-657484703.html.

5 "Which French, German, and UK Brands Create the Most Loyalty With Their Customer Experience?" at http://blogs.forrester.com/joana_van_den_brink_quintanilha/15-09-28-which_french_german_and_uk_brands_create_the_most_loyalty_with_their_customer_expe.

6 IBM's 2017 Customer Experience Index (CEI) Study can be downloaded at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03818USEN&.

7 "US Consumers Turn Off Personal Data Tap as Companies Struggle to Deliver the Experience They Crave, Accenture Study Finds," at 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.

8 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 7.

9 See note 2.

10 GDPR, Article 4(1): "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

11 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.

12 See GDPR, Article 12(2), 12(6), and Recitals 57 and 64.

13 See GDPR, Article 12(3-4).

14 See GDPR, Article 12(5) and 15(3).

15 "The Million Euro GDPR Question: To What Extent Will EU Consumers Exercise Their Rights?" at https://www.i-scoop.eu/gdpr/eu-consumer-gdpr-rights-attitudes/.

16 SAS commissioned a survey of 1,000 Irish adults in late May 2017. See https://www.sas.com/en_ie/news/press-releases/2017/august/irish-adults-intend-to-activate-new-personal-data-rights.html.

17 Pegasystems surveyed 7,000 consumers across seven EU countries. The report is available for download at https://www.pega.com/GDPR-survey.

18 GDPR, Article 5(2).

19 See for example the barriers to complete erasure of a record discussed in this e-book about Salesforce's Pardot marketing automation system: http://www.salesforceben.com/gdpr-salesforce-ebook/

20 The ICO's Subject Access Code of Practice is available at https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf.

21 Ibid.

About Digital Clarity Group

Digital Clarity Group (DCG) is a research and advisory firm that helps organizations deliver world-class customer experience through partnerships with best-fit technology vendors and digital partners. DCG enables client success by bringing unprecedented transparency to selecting, engaging, and optimizing relationships with digital partners and technology vendors. Its guidance draws on its proprietary data about agency and integrator partner performance, its deep experience with vendor and digital partner selections, and the market expertise of its industry analysts who cover technologies for managing customer experiences. DCG delivers on its mission through its VOCalis customer satisfaction assessment program, its vendor and digital partner selection services, and Partner Finder, a free resource that buyers use to identify qualified digital partners based on key criteria.

Digital Clarity Group serves clients across the ecosystem for customer experience solutions. DCG helps enterprise buyers of services and technologies engage with the optimal set of partners for their digital transformation and customer experience initiatives. DCG helps digital agencies and integrators align their client portfolios with their strongest capabilities and competencies, leading to higher levels of customer satisfaction, repeat business, and performance-based differentiation. DCG helps technology vendors optimize their channel partner programs for successful implementations that deliver sustainable value to customers.

Contact Us

Email:
info@digitalclaritygroup.com
Twitter: @just_clarity

www.digitalclaritygroup.com