

Don't Waste Your GDPR Effort on Narrow Compliance



Summary

GDPR is a big deal. In a narrow sense, GDPR is about compliance. However, the ultimate objective is to enable more digital activity. GDPR is one of a number of European Union (EU) initiatives designed to achieve a more comprehensive, seamless, and deeper single digital marketplace across the EU. This ebook will cover off-key compliance points on GDPR. The primary recommendation is that organizations ensure their GDPR programs go beyond a focus on compliance and ensure the program is additive to facilitating digital activity and their digital transformation strategy. The good news for any global business covered by the new GDPR regulation is that GDPR represents an opportunity. The fundamental drivers of the regulation are to promote digital activity, and organizations should be using GDPR to gear up to take more share of that bigger digital marketplace.

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.

– European Commission

Couchbase enables digital customer experiences for many of the world's leading companies.
[Contact us](#) us to boost your digital strategy.



The ebook briefly covers the generic attributes needed for digital transformation and activity (e.g., technology, process, people) and also the key steps in a digital technology transformation process, discussing areas like embedding agility. The ebook also outlines the ideal profile and drivers for the new data protection officer. This essential role should be more than the guardian of GDPR compliance but a key advisor and strategic voice – not only on privacy but also the wider customer experience and vision on digital activity. Within this overarching framework the key do's and don'ts for a GDPR program are:

- 1. Do undertake an organization-wide assessment of compliance to GDPR**
- 2. Don't just focus on tick-box GDPR compliance**
- 3. Do shine a spotlight: use GDPR to check and boost the organization's digital strategy**
- 4. Don't celebrate on May 25, 2018**
- 5. Do focus on the customer**
- 6. Don't forget the ROI**



Digital transformation

In many respects, we are still in the early stages of the digital transformation journey. Yes, digital has transformed many industries and its impact on key business metrics is already significant. But digital will only continue to become more significant. It is important to note the growing digital market doesn't only represent an opportunity. Many companies that can't interact with their customer digitally will face an existential threat. Companies that do not transform, including on the digital front, face a 1 in 3 chance of failing in the next 5 years. That is up from 1 in 20 only 50 years ago.¹

Successful digital transformation means having the right technology in place, the right processes in place, and the right level of talent in place to both establish a solid foundation for change and to continue evolving your digital efforts over time.

Companies that do not transform, including on the digital front, face a 1 in 3 chance of failing in the next 5 years. That is up from 1 in 20 only 50 years ago.

¹Transformation: Delivering and Sustaining Breakthrough Performance, BCG 2016





The right technology: A singular focus on the technology will not drive change and success. However, the right technology is really a necessary condition for almost every transformation program. In our experience, the limitations of legacy technology to support new – and ever-changing – models of interactions is always one of the first issues that needs to be solved.



The right processes: Agile is the only way to go simply because there is no fixed endpoint in the digital journey and changes and disruption are simply part of the general environment. Agile applies well beyond the straight “DevOps” model and needs to be overlaid to the wider governance and decision-making across the business.



The right people: On the talent side, you need the right business and technical talent in place to be able to support new digital markets, quicker decision-making, and continuous learning including learning from failure. In a broader sense, the organization needs key decision-makers ready to challenge the status quo and champion cutting-edge change.

There are no clear and unambiguous answers or requirements for our digital future. Across the technology, process, and people arena, the ability to operate agilely is a critical underlying capability. On the technology piece, it is important that the product and solution meet a specific set of requirements at a point in time. However, what is more important is that the product and technology support flexibility and agility both in its functional and nonfunctional capabilities and also fits within the wider technical architecture of the business.



GDPR requirements and the single digital market

There is an opportunity to ensure compliance with GDPR and add value to the wider digital strategy. Given the overarching objective of GDPR is to enhance digital activity (in the single market), then surely GDPR programs should be additive to this objective. Organizations are increasingly focused on the customer, their customer data, and the customer experience. Organizations should add the GDPR requirements into their general commercial efforts to understand their customers in totality and generate insight. The opportunity is there to both focus on the customer and ensure compliance.

There is no endpoint here. May 2018 (the date GDPR comes into effect) is a useful milestone and businesses need to ensure compliance. However, as with other parts of a digital program, organizations need to support a set of requirements at a point in time but also be able to evolve and be agile as the requirements change. Tactically, there will be adjustments to the GDPR requirements going forward as it beds in and as elements are clarified and tested. This could cover everything from what constitutes personal information or sensitive information through to the exact scope of the various different rights applying to individuals and their own data.

Generally, expect no let up in the rate of change in the digital and commercial world. In many respects new innovations, technology shifts, and customer preference changes will lead to both foreseen and unforeseen interactions and activity in the digital space. Organizations need to be able to respond as these shifts occur in order to be able to do business in that market. As an almost secondary consideration, these changes in the market will often flow back and shift the exact nature of what is needed or what it means to be GDPR compliant.

Given the overarching objective of GDPR is to enhance digital activity, then surely GDPR programs should be additive to this objective.



Functional security highlights carved out from the GDPR: Organizations need to be able to cover these functional areas in a GDPR compliance process context. As part of the mapping of data and data use, these capabilities are highlighted with regard to securing data or ensuring other compliance requirements:

Encryption	GDPR considers encryption as one of the core techniques to render the data unintelligible to any person who is not authorized to access the personal data
Anonymization	Data anonymization is the technique of completely scrambling or obfuscating the data
Pseudonymization	Pseudonymization refers to reducing the linkability of a data set with the original identity of a data subject
Minimization	GDPR recommends minimizing the collection and retention of personal data as much as possible to reduce the compliance boundary
Privileged access controls	GDPR implies need for controlling privileged users who have access to the personal data to prevent attacks from insiders and compromised user accounts
Fine-grained access control	GDPR recommends adopting a fine-grained access control methodology to ensure that the personal data is accessed selectively and only for a defined purpose
Audit activity	GDPR mandates recording or auditing of the activities on the personal data
Monitor: alerts	GDPR also mandates timely notifications in case of a breach – 72-hour breach notification is one of the core alerting requirements



KEY DO'S 
AND DON'TS 





Do undertake an organization-wide assessment of compliance to GDPR

This one is a pretty obvious “do” as the new regulation requires that organizations undertake systematic compliance checks of their current and planned state versus the new regulations. In a nutshell, assessing what data the business has, where the data is stored, and how the data is used/will be used. Given the importance of the regulation and its broad scope and potentially significant penalties, **global organizations need to get on the right side of the regulation and get this done.**



Don't just focus on tick-box GDPR compliance

Organizations will need to comply with GDPR but compliance with GDPR won't necessarily **add a single dollar/euro to the bottom line, improve customer satisfaction, or impact any other critical KPIs that the business operates to.** As GDPR is an enabling component of the single digital market, ensure GDPR investments and effort is also aligned with the overarching goal and KPIs: **enabling an organization to increasingly digitally interact with consumers and businesses.**





Do shine a spotlight: use GDPR to check and boost the organization's digital strategy

If you are interacting with consumers or businesses in the EU, **the board and the C-suite should be reviewing and assessing the organizational readiness to ensure GDPR compliance.** Use that senior-level scrutiny and focus to **not only drive through the GDPR program but enable a wider health check of the entire organization's digital strategy.**



Don't celebrate on May 25, 2018

May 25, 2018 is a really important date and organizations will need to be compliant with GDPR. **But it is a waypoint, not the endpoint.** The regulation will both be clarified and evolve over time and consequently compliance will, in effect, evolve as the regulation beds in. More importantly, **digital activity will evolve over time** as user preferences shift and technology changes. Organizations need to ensure they have the agile underlying **building blocks across technology, process, and people to continue servicing these evolving digital interactions over time.**





Do focus on the customer

At its core, GDPR is focused on the individual consumer, giving them a consistent framework and stronger rights to protect their privacy in the digital age. **Digital leaders have a laser-like focus on the customer and the customer experience** as users interact with their brands. Use GDPR to **assess how customer data, privacy, and trust form part of the overarching customer experience (segment by segment, market by market) and determine how organizations can leverage that data and trust component to boost customer satisfaction.**



Don't forget the ROI

It might be easy to justify resources and investment on the basis of regulatory compliance and simply flag the eye-watering penalties of up to 20 million euros or 4% of global turnover. **If these resources and investments only ensure compliance, that is a wasted opportunity.** By examining your efforts more holistically beyond the immediate impact of GDPR compliance and within context of your overarching digital strategy, organizations can maximize their investment of time and resources while also better positioning the organization to drive forward the digital agenda.

Couchbase enables digital customer experiences for many of the world's leading companies.
[Contact us](#) us to boost your digital strategy.



GDPR regulation requires certain organizations to appoint a data protection officer (DPO) whose core responsibility is to ensure GDPR compliance. Here is a pen portrait outline of a strategic DPO that will add more value into the organization:

New persona in the enterprise – The data protection officer

Title: Data Protection Officer

Reports to: Board

Previous titles: Chief Information Security Officer (CISO),
Chief Security Officer (CSO), VP Security & Networking

Evaluation

- Ensuring core compliance with GDPR regulations across the organization
- Evangelizing, enhancing, and embedding customer-centered and privacy-centered programs across all organizational areas

Triggers

Do say: “Customer trust is a foundation stone of digital interactions.”

Don’t say: “Your team gets in the way of doing business.”

Buying cycle

Increasingly involved in decision-making around scope, select, and buy

Reservations

- Has concerns about vendors overreaching
- Unsure whether privacy and customer are truly at the core of the vendor pitch

Responsibilities

- To inform and advise on obligations pursuant to GDPR
- To monitor compliance with GDPR
- The assignment of responsibilities, awareness-raising, and training of staff
- Provide advice of the data protection impact assessment on processing activities and monitor performance
- Contact point for the supervisory authority and cooperate with the supervisory authority
- Plus CSO/CISO responsibilities

Personal drivers

- Ensure organizational readiness for GDPR on May 25, 2018
- Ensure ongoing support and compliance for GDPR as the business evolves
- Ensure GDPR program is additive to overall business objectives and digital strategy
- Move beyond a technology and guardian mindset/persona and be a strategic and trusted advisor for the business

Features

- Customer and privacy-centered processes and features (e.g., privacy by design)
- Best-in-class security features and dev/design processes
- Agility – demonstrable technology, process, and people sets to meet changing and uncertain business and regulatory requirements
- Fit within security and information ecosystem

Types of content and tactics




- Content which is referenced and validated by peers, analysts, other credible third parties
- External certification
- Strong thought leadership where security or privacy is layered with a business and strategic overlay



General Data Protection Regulation fast facts

	Date: Takes effect May 25, 2018
	Objective: One of 16 initiatives to facilitate the single digital market across Europe
	Purpose: Gives individuals in the EU stronger rights, empowering them with better control of their data and protecting their privacy in the digital age
	Territorial scope: Any organization established in the EU and any organization based outside the EU is subject to the GDPR if it either: (a) offers goods or services to EU data subjects; or (b) monitors the behavior of EU data subjects



	<p>Personal data: Any information relating to an identified natural person ... who can be identified, directly or indirectly, 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</p>
	<p>Organizations impacted: Both data controllers (those who determine the purpose and means of processing personal data) and data processors (those that process personal data on behalf of the controller) of personal data originating in the EU or of EU residents, regardless of the location of the business</p>
	<p>Penalties: Up to 20 million euros or 4% of group worldwide turnover (whichever is greater) against both data controllers and data processors</p>





Key changes from current state:

- ▶ Creates consistent implementation and a baseline across EU countries and verticals
- ▶ Detailed and extended definition of personal data, including relating to digital activity
- ▶ Increased and clarified territorial scope (extra-territorial applicability)
- ▶ Big penalties - up to 20 million euros or 4% of turnover
- ▶ Consent: needs to be unambiguously opted in, clear, and explicit
- ▶ Mandatory breach notification requirements
- ▶ Subject's rights codified: right to access data/subject's right to be forgotten/subject's data portability
- ▶ Overarching privacy by design
- ▶ Single point of contact/responsibility: data protection officers

More information visit:

www.eugdpr.org

ico.org.uk



Conclusion

Couchbase enables digital customer experiences for many of the world's leading companies.

[Contact us](#) us to boost your digital strategy.

About Couchbase

Couchbase's mission is to be the data platform that revolutionizes digital innovation. To make this possible, Couchbase created the world's first Engagement Database. Built on the most powerful NoSQL technology, the Couchbase Data Platform offering includes Couchbase Server and Couchbase Mobile and is open source. The platform provides unmatched agility and manageability – as well as unparalleled performance at any scale – to deliver ever-richer and ever more personalized customer experiences.

couchbase.com

The information in this document may not be construed or used as legal advice about the content, interpretation, or application of any law, regulation, or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of any vendor's products or services.

