2019

dotCMS White Paper

GDPR Compliance: Everything You Need To Know

dotcms

What is GDPR & Who Does it Affect?

The General Data Protection Regulation (GDPR) is a **new legislation that was developed and approved by the European Parliament, the Council of the European Union and the European Commission.** It will be rolled out and enforced starting on May 25, 2018[1]. By that date, companies that collect personal data from their EU customers or clients must be compliant with the various facets of GDPR to avoid heavy fines and legal action.

In short,

GDPR seeks to put an end to brands treating consumer data as a corporate asset, & compels them to see their possession of consumer data as a privilege that the consumer has total & continuous control over.

Whereas in the past corporations have managed to get off relatively lightly for major data breaches, data misplacement and unsolicited data usage, **GDPR will require corporations to explicitly ask for consumer permission for anything pertaining to the collecting, storage, usage of their data.** Plus, organizations will be held to account for any data that is held or handled incorrectly, or without consent.

With fines of up to €20 million being a possibility, the ramifications of falling short on GDPR compliance are potentially huge. And yet, a 2018 study[2] has revealed that **only 33 percent of global brands have a plan in place to comply with the EU legislation in time** for the May 25, 2018 deadline.

European companies are statistically better prepared, with 60 percent indicating they have a compliance plan in place. However, other markets have lagged behind, with significantly less companies showing signs of readiness for GDPR including Africa and the Middle East (27 percent), the Americas (13 percent) and Asia-Pacific (12 percent).

According to

– Herwig Thyssens

ICT director and Head of T-Trust at T-Systems Belgium[3],

“[brands] need to understand that GDPR is not just a project that needs to be implemented, but something that needs to be maintained for the life of the business.”

Clearing Up GDPR Misconceptions

Despite the looming GDPR deadline, there is still confusion over who will be aff ected by the legislation. In fact, **just 47 percent of U.S.- based IT professionals know where they stand on GDPR[4],** indicating a sizeable knowledge gap on what is a global digital landscape changing legislation. With that being said, let's clear up some misconceptions:

01. GDPR is just for Europeans

GDPR may be a European legislation, but that doesn't mean only Europe-based companies are in the crosshairs.

Any organization interacting with EU citizen data will need to be GDPR compliant,

wherever in the world they may be based.

For example, a China based eCommerce company that has no European office, but delivers goods to Europe anyway, will need to be GDPR compliant. It's also worth noting that, despite Brexit, EU consumer data will also encompass UK citizens[5].

Although Brexit means that the UK will no longer consider itself a part of the EU, the UK government has decided to embrace the legislation.

02. GDPR is About Curbing Big Business

While GDPR does tighten up data protection protocols, **the legislation's aim is to empower the consumer,** not hinder big business.

GDPR essentially allows your customers to control their data, wherever it may be. Thus, **data is no longer solely a corporate asset that can be exploited, misused or sold on at will.** Similar to how politicians are beholden to their constituents when deciding policy, your company is beholden to your customers when using their data[6].

Here's a brief look at how consumers will regain control over their data post-GDPR:

- Customers need to opt-in to sharing data, rather than opting out.
- Pre-checked forms are no longer acceptable.
- Using customer data for purposes other than declared is no longer acceptable.
- Acquiring customer data to sell to advertisers wantonly is no longer acceptable.

- Customers need to opt-in to sharing data, rather than opting out.
- Pre-checked forms are no longer acceptable.
- Using customer data for purposes other than declared is no longer acceptable.
- Acquiring customer data to sell to advertisers wantonly is no longer acceptable.

03. GDPR is Bad News

Many companies wince at the word GDPR because of the strict guidelines the legislation imposes. But in reality, many of the provisions within GDPR are common sense and, if your business is already using data processing best practices, there won't actually be too much work to do.

Furthermore, **GDPR will directly result in companies collecting and using 'cleaner' data.** For example, your email list will be made up of fewer subscribers, but every single subscriber you do retain will have explicitly given their permission to receive your marketing messages.

As you might imagine,

purifying your data in this way may result in higher conversion rates.

On another note, brands who attain GDPR compliance will be able to use their legal and consumer-friendly status to differentiate themselves from their non compliant competitors. **Being able to proudly announce your GDPR compliance, despite the strict protocols in place, will give your customers a new lease of confidence in your brand, and the way it manages data.**

With these various GDPR benefits at play, it's not totally surprising that many IT professionals are looking forward to the arrival of GDPR, despite the stiff preparation process. Surveys carried out in the UK and European Union[7] show that

65 percent of UK-based IT professionals and 59 percent of EU-based IT professionals are in favor of GDPR.

Contrastingly, a mere 37 percent of U.S. based IT professionals said they are in favor of the impending regulation. That lower approval rate, however, may have a lot to do with the aforementioned knowledge gap this same study uncovered among U.S.-based IT professionals.

GDPR: Key Sections At a Glance

Understanding the key sections of GDPR will come in handy when you take the steps towards GDPR compliance outlined later in this document.

Data Subjects, Controllers & Processors.

To truly understand the details of GDPR, you need to be familiar with three key terms that are used throughout the legislation to define roles and their resulting regulations.

The following definitions can be found in Article 4 of GDPR[8]. Understanding the key sections of GDPR will come in handy when you take the steps towards GDPR compliance outlined later in this document.

Data Subject:

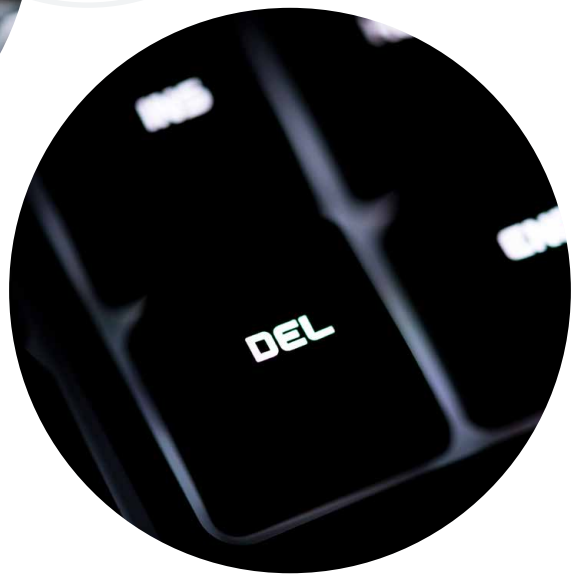
A ‘data subject’ is an identified or identifiable natural person — which often translates into the **average consumer GDPR seeks to protect and empower the data subject.**

Controller:

A ‘controller’ is the natural or legal person, public authority, agency or similar body which, alone or jointly with others, **determines the purposes and means of the processing of personal data.**

Processor:

A ‘processor’ is a natural or legal person, public authority, agency or similar body which **processes personal data on behalf of the controller.**



The Cusomer's Right To Be Forgotten

Also known as the right to erasure, data subjects will have

the power to request that their data is totally deleted — a request that the company in questions must fulfill

unless there is a clear and legal need for the company to retain the data[9].

For instance, a customer cannot request that a power company delete his or her data in he middle of the winter because shutting off the power could have disastrous effects for the individual.

However, a customer switching phone companies could request that the soon-to-be-replaced company delete his or her data before switching to a new company and phone plan.

GDPR Legislation

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and

the controller shall have the obligation to erase personal data without undue delay where

[certain grounds apply][10].

Tellingly, a recent PEGA survey[11] revealed that **82 percent of consumers would choose to exercise their right to be forgotten at some stage.**

Expanded Consumer Rights

On top of the consumer's right to be forgotten, data subjects also have the following rights over their data, each one boasting its own set of laws and clauses:

01. Right to be Informed:

A set of consumer rights aimed at increasing transparency.

02. Right of Access:

Consumers must have complete access to their personal data and supplementary information.

03. Right to Rectification:

In cases of error, the data subject has the right to have personal data rectified.

04. Right to Restrict Processing:

Data subjects have the right to 'block' or suppress processing of personal data.

05. Right to Data Portability:

Data subjects must be given the ability to export or download their data.

06. Right to Object:

Consumers have the right to Individuals have the right to object to things like direct marketing (including profiling) and processing for purposes of scientific/ historical research and statistics.

07. Rights Related to Automated Decision Making:

In certain circumstances, controllers and processors who practice automated decision making like profiling or consumer segmentation will need to give data subjects sufficient information about the process and give them simple ways to request human intervention or challenge a decision.

According to Article 33 of GDPR, if a data breach occurs, responsible parties have just 72 hours to report the incident to the relative authority in their country or region.

Mandatory 72-Hour Data Breach Reporting

GDPR Legislation:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons[12]."

The Requirement of Explicit & Ongoing Consumer Consent

Companies have traditionally collected information from users via web forms. These forms may ask for user's addresses, email addresses, phone numbers and so forth. **Under GDPR, all information will need to be explicitly asked for.**

Users will need to opt-in to provide information, rather than opt-out as they usually have done in the past.

An individual can also request that his or her data is deleted from company servers. Consent must be clearly and explicitly expressed[13].

GDPR Legislation

"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to [the] processing of his or her personal data...

The data subject shall have the right to withdraw his or her consent at any time.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal[14]."

New Data Processing Protocols

Depending on the level of data processing your company is responsible for, a data protection impact assessment may need to be carried out[15].

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons,

the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A single assessment may address a set of similar processing operations that present similar high risks[16].”

International Data Transferring

Under GDPR, transferring data outside the EU will be prohibited.

For the purpose of GDPR, the UK is considered to be a part of the EU.Transfers will only be allowed under GDPR if:

- They are made by private companiesendam,
- Are single transfers
- The data is limited to the individuals who are required to access it (also known as the principle of least privilege)
- Are necessary for business operations
- The data is secured to protect it

GDPR Legislation

“A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country,

a territory or one or more specified sectors within that third country, or the international organisation in question

ensures an adequate level of protection.”[17]

GDPR Fines: The Dangers Of Non-Compliance

If your company does not comply with GDPR, but is legally required to do so. There are two tiers of administrative fines that can be levied[18]:

01. Lower Tier:

Up to €10 million, or 2 percent of annual global turnover – whichever is higher.

02. Higher Tier:

Up to €20 million, or 4 percent of annual global turnover – whichever is higher

Generally speaking, the lower tier will apply to 'lesser' infringements, whereas major infringements will be more deserving of the higher tier. Naturally, the circumstances of each case will need to be weighed up, and deliberate or malicious data handling will, for example, be taken more seriously than accidental data leaks.

When deciding whether to impose a fine and the level, the ICO must consider[19]:

- **The nature, gravity and duration** of the infringement;
- **The intentional or negligent character** of the infringement;
- **Any action taken by the organisation to mitigate the damage** suffered by individuals;
- **Technical & organisational measures** that have been implemented by the organisation;
- **Any previous infringements** by the organisation or data processor;
- **The degree of cooperation** with the regulator to remedy the infringement;
- **The types of personal data involved;**
- **The way the regulator found out** about the infringement;
- **The manner in which the infringement became known** to the supervisory authority, in particular whether and to what extent the organisation notified the infringement;
- **Whether, and, if so, to what extent,** the controller or processor notified the infringement;
- **Adherence to approved codes of conduct or certification schemes.**

Needless to say, such fines and legal vulnerabilities could permanently damage or even bankrupt companies.

Worse yet,

the public scandal that comes as a result of being punished would deal damage to the brand's reputation, as well as the reputations of the executives at the helm.

Five Steps Towards GDPR Compliance

Becoming GDPR compliant is a multi-dimensional process that depends on the current state of your data collection, storage and processing protocols. While every situation is unique, we've compiled some of the fundamental considerations you need to make in the build up to the GDPR deadline on May 25, 2018.

01. Understand GDPR's Legal Framework

Before taking any action, it's vital that your organization's leadership reads and understands GDPR.

It's advisable to bring in legal assistance to help contextualize the legislation for your industry & also for your company specifically.

Properly understanding how GDPR affects your company will help you avoid actions that you didn't need to do, and to act faster on areas that you previously thought were taken care of. Plus, it ensures no part of the regulation slips past you, resulting in incomplete compliance.

02. Audit Your Existing Data Processes

The next step is to **evaluate the way your brand collects, manages and uses consumer data.** The following questions can help you along the way:

- Through what channels do you collect consumer data?
- How and where is that data stored?
- How does your business process it?
- What data do you use, and what data sits idle?
- Is there a step in the process where you are unaware of the state or security of your data?
- Do you send data to remote workers and outsourced operations?
- Do you send and receive data from third party companies like payment processors, document management systems, and the like?
- Has your business ever been the target of a data breach or hack?

If you don't know the answers to this non-exhaustive list of vital data protection questions, there's no way to know whether your company is GDPR compliant or not.

Thus, they will all need to be considered if you want your company to become — and remain — GDPR-compliant.

03. Be Open With Customers Regarding Their Data

If your user agreements, privacy policies and consent tick boxes are not clear, make them clear.

Seek to inform your customers why you need their data, what you will use their data for, and their rights concerning their data.

You should also give clear instructions to your customers on how the can access their data, export it and request for it to be modified or deleted.

After GDPR comes in, you won't be able to rely on fine print or long, technical user agreement forms in order to convey these messages. The user needs to be spoken to in clear, concise terms. If need be, rewrite your user agreements so that the layperson can understand them.

Here is the difference between a clear and concise agreement and legalese.

- **Bob gives Alice an orange.The outcome here is very clear.**
- **Now, the legalese. Bob gives Alice an in-season orange-tinged hesperidium, consisting of the rind, seeds and flesh.**

In both these statements, Bob gives Alice an orange. However, only the first iteration of the scenario would be simple and concise enough to be considered acceptable under GDPR.

04. Appoint a Data Protection Officer (DPO)

GDPR requires some organizations appoint a data protection officer (DPO) — **an individual who should oversee an organization's data protection strategies and compliance programmes.**

A DPO becomes obligatory[20] when the organization in question is:

- **A public authority** (except for courts)
- **Carrying out out large-scale systematic monitoring of individuals** (like online consumer behavior tracking)
- Carries out large-scale processing of special categories of data or data relating to **criminal convictions and offenses.**

It's worth noting however that the term 'large scale' does not necessarily mean hundreds of thousands of data subjects[21] — so do your homework on that front. Also, while only some organizations need a DPO, appointing a DPO will be seen as good practice by GDPR regulators and the public.

Five Key Duties of a Data Protection Officer

Some organizations have already hired, or are planning to hire new employees for the DPO role, while others are expanding the roles of existing employees, like Chief Privacy Officers. There is no recommended work history or experience that prospective DPOs should have, although

Article 39 of GDPR provides a list of the minimum tasks a DPO must perform,

which we have laid out below[22].

01. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

02. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

03. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35[23].

04. To cooperate with the supervisory authority;

05. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

While carrying out the tasks above, GDPR states that the DPO should have, **"due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing".**

05. Prepare for Data Breaches

Data breaches are an unfortunate part of the modern, connected world. Mammoth corporations have succumbed to breaches in the past, and it will be no surprise when such incidents strike again.

As seen with the recent Equifax data breach[24], companies do not always make immediate public statements when they are hacked[25], instead, they choose to sit on the information for some time.

However,

GDPR requires that brands take every measure possible to avoid breaches in all their forms, and, as previously mentioned, to notify the relevant body within 72-hours.

That means publicly admitting digital defeat at the hands of hackers, which could be financially and reputationally costly.

With that in mind, your best bet is to **be as prepared as possible with protocols designed to limit damage during an attack, staff training and drills,** developing internal cyber security intelligence, as well as an emergency press release — just in case.

Get Help Preparing for GDPR

GDPR compliance will be no walk in the park for any company, but with the right technologies in place, managing data in compliance with GDPR can suddenly become second nature. Moreover, partnering with a technology vendor that understands the serious implications of GDPR could be the difference between compliance and sky-high fines.

Here at dotCMS, we're either already meeting, or are close to meeting our GDPR obligations in time for the May 25, 2018 deadline. We have a **strong foundation of certified security and privacy controls** by design and will continue to make product enhancements to aid our enterprise customers meet that deadline with us.

Our approach to GDPR compliance can be broken down to six point[26]:

01. A Strong Foundation of Security & Privacy Compliance.

We've implemented a set of **certified security processes and controls to help protect the data entrusted** to us through the dotCMS Security and Privacy Policies. This helps us comply with several security and privacy certifications, standards, and regulations, including SOC-2, ISO 27001, and the EU-U.S. Privacy Shield.

02. Privacy by Design

Our mission is to help you responsibly unlock the power of data. dotCMS has a long-standing practice of incorporating a proactive product development effort, also known as "privacy by design." For example, **dotCMS has the ability to obfuscate Internet Protocol (IP) addresses and allow individual-level opt-outs.**

03. Compliant Data Transfer

dotCMS is aligned to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks for customer-related data. This provides our customers with the option of relying on these frameworks or entering into Standard Contractual Clauses for the transfer of data from the EU to the U.S.

04. Watertight Contract Terms

dotCMS has updated our agreements with customers and vendors to account for GDPR requirements.

05. Records of Processing

dotCMS is working to more formally document the privacy practices we have in place to comply with the enhanced record-keeping requirements.

06. Product & Process Innovation

dotCMS is constantly listening to its customers and

looking for ways to simplify & further automate our product & service offerings to better support their GDPR needs.

We have created the office of Chief Information Security Officer to focus on providing the mandated requirements of the GDPR, and to allow the product to maintain the utmost standards to security and privacy of consumers.

With our own digital ducks in a row, dotCMS is better able to assist its global partners and clients with their own GDPR compliance issues in time for the deadline.

Thus, dotCMS clients don't just get a digital experience platform that can be help any brand achieve GDPR compliance, but they also get the expertise & thought leadership that comes as part of the support every dotCMS client gets.

Complimentary Evaluation Support

dotCMS offers a variety of tactics to test-drive and proof out your key use-cases around your personalization strategy. It is our investment and helps you to evaluate dotCMS effectively, way beyond shiny product demos and slick sales presentation.

More on our evaluation support
Here>>>

About dotCMS

dotCMS is a leading, open source content and customer experience management platform for companies that want innovation and performance driving their websites and other content-driven applications. Extensible and massively scalable, both small and large organizations can rapidly deliver personalized and engaging content across browsers, mobile devices, channels, second screens and endpoints -- all from a single system.

Founded in 2003, dotCMS is a privately owned US company with offices in Miami, Florida; Boston, Massachusetts and San Jose, Costa Rica. With a global network of certified development partners and an active open source community, dotCMS has generated more than a half-million downloads and thousands of implementations and integration projects worldwide. **Notable dotCMS customers include:** Telus, Standard & Poors, Hospital Corporation of America, Royal Bank of Canada, DirecTV, Thomson Reuters, China Mobile, Aon, and DriveTest Ontario.

Miami
3059 Grand Av.
Miami,FL,33133
U.S.A

Boston
200 Portland St.
Boston,MA,02114
U.S.A

Heredia, Costa Rica
Eurocenter
Primera Etapa, 2nd Floor
106 Heredia, Costa Rica

ON-DEMAND DEMO

dotcms.com

+1-305-900-2001

sales@dotcms.com

References

1 Eugdp.org (2018), **"What is GDPR"**

2 Eugdp.org (2018), **"What is GDPR"**

3 ComputerWeekly (2017), **"GDPR Impact Complex Warns Expert"**

4 Spiceworks (2017), **"Many Companies Unprepared for GDPR"**

5 ComputerWeekly (2017), **"GDPR Impact Complex Warns Expert"**

6 CMSWire (2017), **"Your 5-Step GDPR Readiness Plan"**

7 Spiceworks (2017), **"Many Companies Unprepared for GDPR"**

8 GDPR Info (2017), **"Article 4"**

9 CMSWire (2017), **"Your 5-Step GDPR Readiness Plan"**

10 GDPR Info (2017), **"GDPR Article 7"**

11 PEGA (2017), "**EU Consumers Poised to Take Back Control of Personal Data"**

12 GDPR Info (2017), **"GDPR Article 33"**

13 co.org.uk (2018), **"Consent"**

14 GDPR Info (2017), **"GDPR Article 7"**

15 Ico.org.uk (2018), "Data Protecti on Impact Assessments"

16 GDPR Info (2017), **"GDPR Article 35"**

17 Ico.org.uk (2018), **"International Transfers"**

18 GDPR Info (2017), **"GDPR Article 45"**

19 GermServ (2017) **"A Guide to GDPR Fines"**

20 IT Governance (2017), **"Who Should Fill The DPO Role"**

21 Gartner (2017), **"Gartner Says Organizations Are Unprepared for GDPR"**

22 GDPR info.eu (2017), **"Tasks of the Data Protection Officer"**

23 GDPR Info, (2017) **"Article 35"**

24 Time (2017), "**The Equifax Hack Affects 143 Million People. Here's What Makes It Even Worse"**

25 Observer (2017), **"Equifax Said Execs Didn't Perform Insider Trading During Data Breach"**

26 dotCMS (2017), **"GDPR Policy"**