Kentico

GDPR Compliance and Your CMS

Reliable Customer Data for Better Marketing Results

GDPR Compliance and Your CMS: Reliable Customer Data for Better Marketing Results

Content management systems, particularly those that provide capabilities for digital marketing and e–commerce, sit in the middle of continuous visitor and customer activities on websites and other digital properties. The CMS is often a processing point for large amounts of personal identification information that now must adhere to the privacy regulations of the GDPR.

To better understand how a GDPR–ready CMS helps organizations comply with the new privacy regulations, as well as the other benefits that result, this paper will clarify:

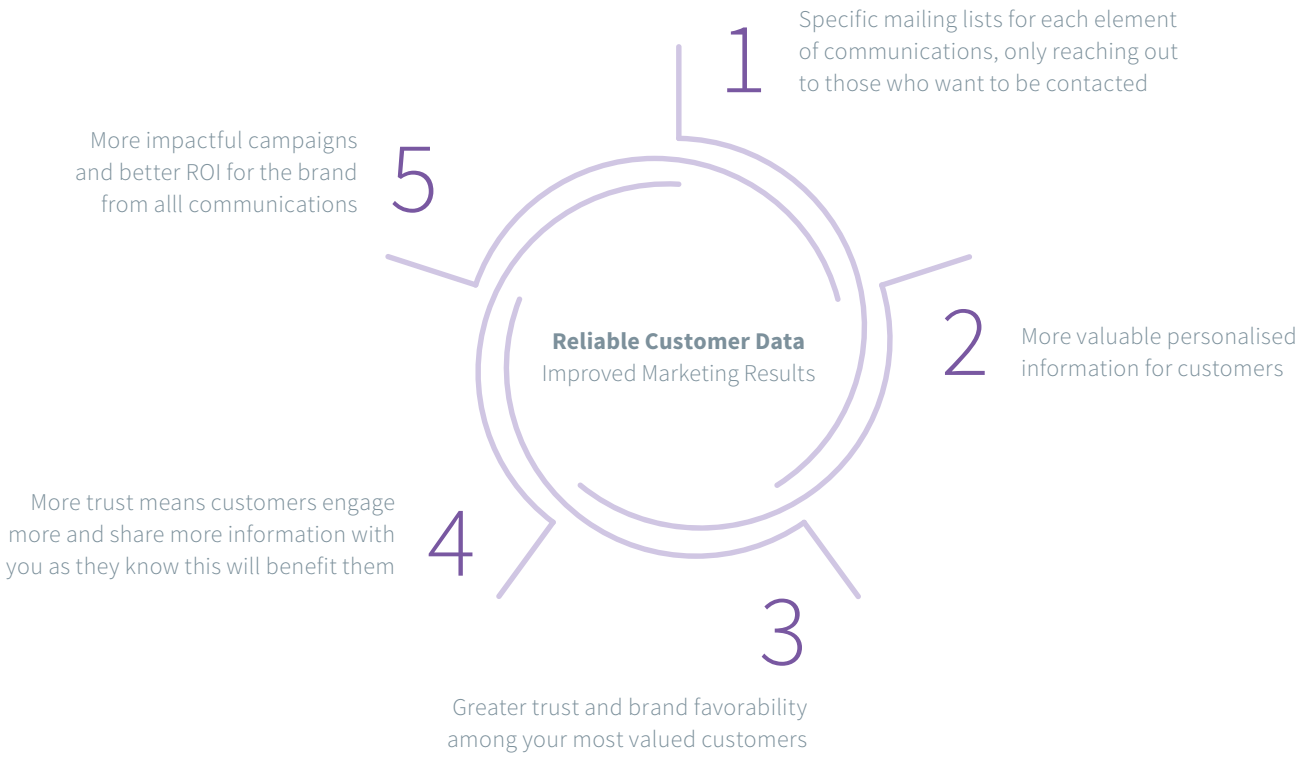
- The real value and benefits for business and marketing that come from the work done for GDPR compliance
- High level points of what GDPR compliance involves
- How GDPR compliance improves the quality and reliability of customer information, which lead to better marketing results
- How marketing and sales will change because of GDPR
- How a GDPR–ready CMS helps with GDPR compliance, which also contributes to better marketing outcomes

GDPR and Customer Information Management

With continuous revelations of data breaches around the world, it should be no surprise that governments are instituting data protection laws to help keep personal information more secure. The EU has mandated compliance with the General Data Protection Regulation (GDPR) by May 25, 2018. The GDPR is set to have significant global impact for many organizations, whether based in the EU or not.

The GDPR has been created to standardize data protection regulations across the EU. The objective is to return control to individuals for their personally identifiable information (PII), while making organizations accountable for how they use and protect personal data. Compliance with the GDPR isn't just a matter for data management professionals. The entire company has the responsibility to understand and comply with the regulation, and, therefore, GDPR education is essential for many groups, including marketing, website management, and mobile apps.

The GDPR will instigate substantial change to how businesses operate, which can also mean new opportunities and benefits for organizations. It forces organizations to handle data more responsibly, something these organizations should have been doing anyway. Internal groups like marketing will now practice better data management, which will result in better quality customer information.



GDPR Compliance Leads to Real Benefits for Marketing and the Business

Organizations have been focused on the extensive work necessary to comply with the GDPR. Compliance is a very important outcome of all that work—but beyond compliance there is also a significant set of benefits for the business and marketing. Many of the benefits revolve around the greatly improved reliability of customer data, particularly for marketing purposes.

Marketers use customer data extensively, but many marketing groups have done a poor job of setting up optimal data management policies and procedures to ensure the quality, relevance, and usability of that data. With the GDPR, entire organizations will now have intelligent approaches to collecting and handling personal data. Implementing better data management and privacy procedures opens the way for organizations to reap greater value from customer data and how it used for a variety of functions, including digital marketing, e–commerce, and customer service.

1 Greatly Improved Customer Trust

Organizations now clearly demonstrate respect for the privacy of their customers and the security of their information. Trust is invaluable and lost easily. It must be earned continuously, particularly in today's digital economy. GDPR compliance gives organizations a significant "trust" stamp of approval.

2 Better Data Quality for Personalization

The buying experiences that customers want depend on the right kind of personalization. Customers have high expectations for accurate personalized experiences, whether through email marketing, e–commerce, or other digital interactions.

3 More Reliable Targeting for Email Marketing

Organizations that send emails only to those prospects or customers who are already interested in products and services (through opt–in consent) ensure that better leads result. Wasted time and resources are eliminated by no longer sending emails to a massive list of names, many of whom will never respond.

4 Quality Leads from Most Marketing Efforts

Prospective customers who have opted in to receive content and communications should produce higher click–through rates and sustain quality engagement throughout the sales cycle, which will likely result in more sales.

5 Enhanced Cross–Team Collaboration

Cross-functional collaboration is essential to ensure consistent GDPR compliance. With such collaboration processes now in place, smoother hand-offs between marketing, sales, and customer service will help keep prospective customers engaged and on track throughout the sales process.

6 Marketing Innovation

GDPR practices will spur new ways of marketing, including ways to work with prospective customers that don't require personal data. Organizations have been obsessed with collecting personal data from every engagement, without considering if they really need the data.

“Bill of Rights” for Personal Information

GDPR regulations address any information that can identify an individual, no matter how it is collected. Companies must become proactive in developing compliant procedures for handling customer personal data and responding agilely to customer rights under the GDPR. This returns the benefit of showing people that you respect them and want to use their personal information wisely, usually leading to increased trust.

Organizations must solicit specific consent from individuals for collecting and storing their information for any purpose. In general, GDPR requirements relate to eight fundamental rights that people now have over their personal information:

Right to be Informed

Clearly worded and easy–to–find privacy policies published by organizations, as well as easy–to–follow methods to respond to customer inquiries quickly.

Right of Access

When a customer requests a copy of their information from a particular organization, it must be sent for free, in a commonly used electronic format, within a month of the request.

Right to Rectification

Organizations must amend incorrect or incomplete information when asked to do so by a customer, in a timely fashion.

Right to Erasure or to Be Forgotten

Organizations must comply with requests from customers to delete their personal information from all systems.

Right to Restrict Processing
Individuals can prevent the use of their data for a particular task or function. But organizations are allowed to keep enough data to be able to do so.

Right to Data Portability
Individuals who have opted in to provide personal data can request that the data be shared with another organization, and this request must be met.

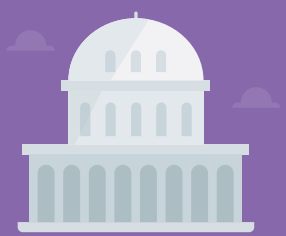
Right to Object
Individuals can object to their data being used for a particular function and can rescind previous consent.

Rights in Relation to Automated Decision-making and Profiling
Individuals are protected from potentially damaging decisions being made without human intervention and without the knowledge of the individual.

Requirements

Rules

Standards



Governance

Compliance

Regulations

Transparency

Policies

Law

Why Global Organizations Must Comply

Every organization must evaluate how it works with personal information related to the EU or UK, regardless of where the organization is located. (The UK is implementing a new Data Protection Act that is very similar to the GDPR.) If an organization handles or controls the personal data of any citizen in the EU or UK, even if the data is processed through a third party, it must comply with the GDPR / DPA, or face serious penalties for the lack of compliance. Depending on the type of violation, fines can go as high as $24 million USD (€20 million) or 4% of global annual revenue (whichever is greater). These big penalties show that the regulators are serious and that companies cannot afford to ignore these regulations.

But organizations can suffer more costly penalties: the loss of customer trust and confidence along with serious damage to the reputation of the organization. Customer trust is difficult to regain once lost. Most data breaches have become headline news over the past few years. It's not unreasonable to expect the same kind of bad publicity for organizations that have failed to meet GDPR compliance requirements. This is the kind of negative press that organizations work to avoid, and can drive away the business of both current and future customers. Even after achieving compliance, such organizations may continue to lose customers who will always wonder if their private information is safe.

Processing Customer Information across Multiple Entities

Organizations have been tasked with creating overall strategies, followed by implementing policies, practices, and processes, to address all of the requirements of the GDPR. Companies that already have good data management teams and systems in place and have implemented decent data privacy measures will find compliance much easier.

Organizations will need experienced data management professionals to design and implement systems at the corporate level and to coordinate efforts with departmental teams. Groups within organizations will have specific responsibilities for compliance that must dovetail with the overall plan. Activities related to websites, e–commerce platforms, and marketing that involve customer information must now include data management processes that can be shown to be in compliance.

GDPR has specified two categories for entities that handle customer personal information: the controller and the processor. Controllers are the main organizations that determine the purpose and means of processing personal information, whether or not they directly collect the data from customers. Processors are basically third–party services and agencies who work with data provided by controllers, and can also be the collectors of personal information on behalf of the organization that is the controller.

At the high level, it's the responsibility of the controller to monitor, coordinate, and ensure the compliance of processors. And processors must prove compliance to controllers. Each of these entities is equally liable for meeting GDPR requirements. Proving compliance becomes even more complex due to the increasing digital nature of marketing and business in general. Digital third–party services that process data on behalf of data controllers can include: hosting providers, SaaS and cloud service providers, web developers, and software and app developers.

Changes to the Client/ Agency Relationship

Under the GDPR, marketing and digital agencies are now essentially an extension of their client organizations, simply because the client organization will be held accountable for any work done by an agency that is not following the regulation. Agencies have to prove their compliance both to GDPR oversight functions and to all of their clients. While agencies are often data processors for their clients, they would be prudent to carry out compliance activities as if they were also the data controllers of client data, to ensure thorough management and implementation of their data practices and processes.

Client organizations have the responsibility of full transparency about their use of third–party services and agencies, in terms of their customers' personal information. Client organizations are now partners with agencies and other third parties to answer any challenges from their customers regarding the status and use of personal information.

Agency contracts will now have to include details of how customer data will be handled in compliance with the GDPR, for every kind of work done for the client organization that relies on personal information. Such details include where data is held and who is in charge of it. If agency work includes purchased lists or databases, agencies will have to be able to prove where the customer data came

from and if customer consent was attained for inclusion. Agencies have to ensure that transfers of data between different parties fully protect personal information.

Collaborative partnerships between agencies and clients are critical to identify what data is being captured by clients, where it is being stored and transferred, and how it is being protected—in terms of the client systems that are accessed by agencies for work on behalf of the clients. Such systems include:

- CRM applications, many of which are now cloud–based
- Website or other web interaction applications—often s upported by a CMS, e–commerce platform, digital experience platform
- Digital marketing applications
- Email marketing applications, if not included in the above
- Google Analytics

GDPR Effects on Marketing and Sales

Marketing roles that will likely be affected the most are: email marketing managers, marketing automation specialists, and public relations executives, as well as the marketing technology and data management teams that support them. The GDPR has completely changed how marketers handle data, especially if the marketing group hasn't been practicing good data management and privacy methods.

Since marketing is affected, GDPR compliance also impacts sales teams. For example, companies that rely heavily on email marketing to collect leads (whether or not they are quality leads) will have to change their ways to comply with the GDPR. Before sending emails, marketing must now gain permission (opt in) from potential recipients—for every distinct campaign. This will likely reduce the target pool of people for email marketing. This will also mean that people who opt in are better prospects for the sales process because they are demonstrating interest in the company and products. And if these same people fill out forms for premium content (opt in), they have an even greater likelihood of responding well to sales conversations.

Marketing and sales teams benefit from better collaboration to facilitate the involvement of sales teams much earlier in the lead–nurturing process. With better quality leads from prospects who have purposefully opted in for contact, sales teams have the opportunity to work on relationship–building much earlier in the sale process. This may mean closing deals more quickly.

Five Marketing Automation Pitfalls!

1 Automated Data Management
You need to audit any existing, updated, and future automated data management processes as well as their outputs.

2 Reverse IP Tracking
You require explicit consent to track a person's behavior based on their IP address.

3 Lead Scoring
As this is a form of profiling under GDPR, before applying lead scoring, you must obtain explicit consent from data owners.

4 Reactivation Programs
Without valid consent, you cannot email anyone, even when requesting them to reactivate a lapsed opt-in.

5 Disposal of Records
You must delete all database members that you do not have a valid opt-in for.

Specific Marketing Activities That Must Change

Marketing teams must thoroughly review practices for every marketing activity that involves personal information, particularly around consent from people regarding the use of their personal information. Each usage of data must have a separate consent that must be documented. An organization can't collect personal information related to one activity and then assume the organization can use it for anything. Marketing and sales teams have to ascertain that the systems that process personal information will be able to handle requests from customers regarding their rights under the GDPR, including access, deletion, portability, and processing requests.

Email Marketing

Compliance affects all email lists: out–of–date, current, and future ones. Out–of–date lists must be deleted. Organizations will have to devise a process for current email recipients to opt in or out for the continuation of email notifications. Email lists must be updated continuously, and proof of compliance must be readily available. Since this is a lot of work, marketers can use this as an opportunity to engage customers by offering something of reasonable value for overt opting in, such as premium content.

Marketers are required to provide certain information in "re–engagement" emails:

- Why is the company contacting them?
- How did the company acquire their personal details in the first place?
- How they can update their communication preferences or opt out?
- What does the customer get in return for opting in for this particular email?

Purchased Lists and Datasets

For-fee contact lists have become very problematical under the GDPR. Those firms selling customer lists and datasets have to gain consent from everyone on the list within a reasonable time frame and provide documentation of such consent. Organizations that already own lists have to do the same thing. Organizations may well have to abandon purchased lists that cannot be authenticated. Lists and datasets that are no longer used must be deleted.

Cookies and Remarketing

Organizations that use cookies to track online activities for remarketing or other purposes are required to clearly show in their privacy policies that cookies are being used, what information is collected, and for what purpose. Customers or visitors must be able to easily opt out of cookie tracking for each individual use—essentially, people can pick and choose the kind of cookies that are enabled. Under the new rules, just visiting a website for the first time doesn't qualify as consent. Nor do the current cookie pop–up boxes meet the requirements of the GDPR regarding consent. In the case of cookies used for tracking, if visitors have set their web browsers to accept or reject cookies, this may meet the GDPR requirement for consent, since users have to manually activate this setting. But it would be best to consult with legal advisors to make sure.

Not compliant

First name

Last name

Business email

Download Trial

By signing up to a free trial of Kentico CMS, you agree to our Terms and you have read our privacy policy. You may receive email updates from Kentico and you can opt out at any time.

GDPR compliant

First name

Last name

Business email

By signing up to a free trial of Kentico CMS, you agree to our Terms and privacy policy.

Please subscribe me to the Newsletter.

Download Trial

Web Forms

Web forms can no longer include pre–checked boxes since implied consent is no longer acceptable under the GDPR. Visitors to websites must overtly opt in for anything offered. Web forms must be designed to make clear how visitors opt in or not.

Web Analytics

Web analytics may have greater restrictions now that people have the right to opt in or out. Organizations may be able to utilize their notices of how cookies are used as the means to record consent (or the lack of consent) for personal information to be used in web analytics, and to show how this information may be shared with third–party organizations. If this approach is selected, then include a link to the central site or portal for consent management, so visitors can find further information on their rights.

Even in the common case where web analytics aggregates data for analysis (and doesn't process data at the level of personal information), consent may be required if data is also segmented, which provides a certain factor of identity.

Pseudonymous data may also come into play to help web analytics in regards to GDPR regulations. When data has been manipulated in ways that remove direct characteristics of identity, it has been pseudonymised. There is usually a "key" composed of one or more unique characteristics that map back to a particular customer or visitor. The key is stored separately from the pseudonymised data to better secure the data if a breach should occur. This approach must be carefully executed with considerable assessment of its security.

For organizations using Google Analytics, Google does make the claim that it has been working to be GDPR compliant by May 2018. Organizations should investigate how Google will prove compliance and should discuss with legal advisors the pros and cons of using Google Analytics.

Web Hosting

Organizations that host or support websites and CMS projects will have to make certain changes to client agreements regarding visitor personal information and how it is used and managed. Web hosting organizations will have to detail how they will comply. They must specify where visitor data is stored and what privacy measures are in place to protect personal data against alteration, loss, and unofficial processing.

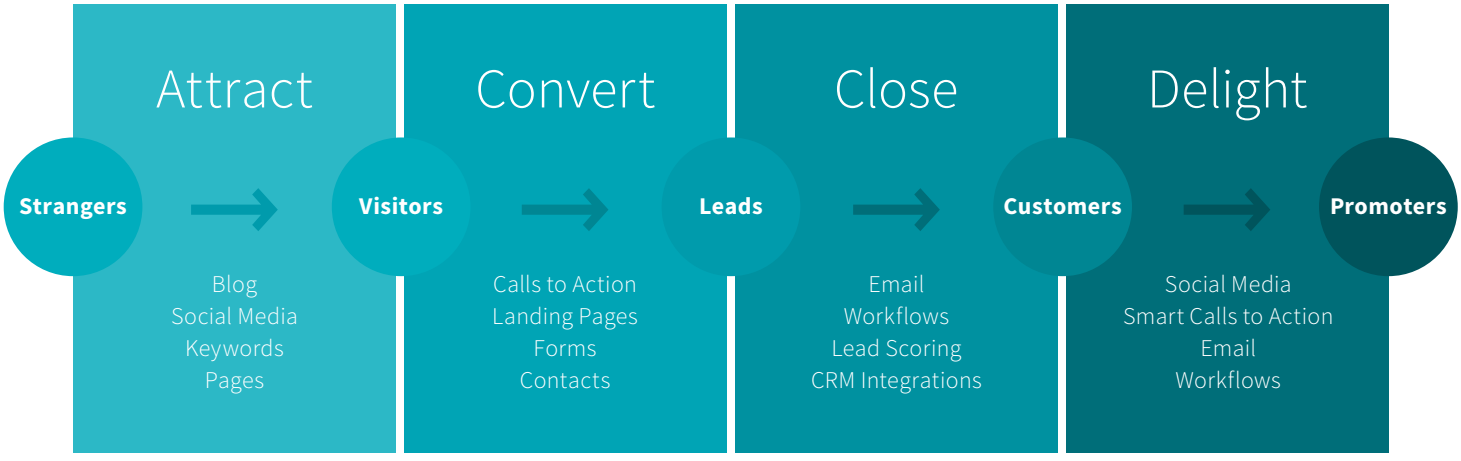
The web hosting organization should clearly state in their terms and conditions that the information is owned by the client and will be shared with third parties only if the client gives permission. The client then must have permission from visitors to do so. The web hosting organization agrees to adhere to all of the actions required by the GDPR regarding visitor or customer access to personal information and the processes for consent, deletion, and so on.

Privacy Policy Statement

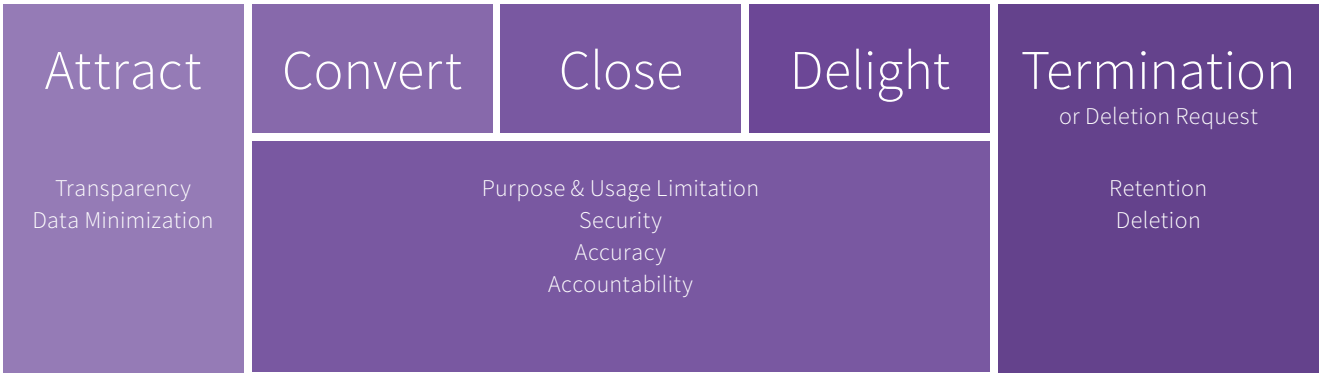
Under the GDPR, privacy policy information must be easily accessed, free of charge, and written in concise clear language that fully explains all privacy aspects. The privacy policy should fully explain organizational practices around privacy. For example, the policy could reveal to website visitors that their personal information may be shared with third parties working with the organization, outline the responsibilities the organization has to protect data privacy in this situation, and show how website visitors can opt out if they so desire.

How GDPR Changes Inbound Marketing Processes

Before GDPR Classic Inbound Marketing Flow



After GDPR Inbound Marketing Flow



Step 1
Data Collection

Step 2
Data Storage and Processing

Step 3
End of the Relationship

Inbound Marketing—Activities to Change or Add:

Web forms and landing pages – For each unique item, visitors must be given the choice of opt–in consent (no more pre–checked boxes). Provide an easily–found link to the policy on:

- Why the organization is asking for the data
- How it will be used
- Opt–in and opt–out rules, as well as other individual rights under the GDPR

Double opt–in approach – This becomes standard for many marketing activities: anytime a visitor completes a form or other request, an email is sent to ask the visitor to confirm the email address and verify consent.

Marketing automation – For each unique consent, visitor information can only be used in the specific way associated with the consent. A new activity requires a new consent. Provide easy access for visitors to opt out whenever they desire.

How a GDPR–Ready CMS Helps with Compliance

Most organizations should have an overall plan for meeting GDPR requirements that has been developed with the input from many teams, including legal advisors. Such a plan should address all systems and processes that handle personal information, including those for marketing and company websites.

Content management systems (CMS) are often an essential component of the digital technology stack that delivers quality visitor and customer experiences on various online sites. A CMS may track, store, and process a great deal of personal and behavioral information related to online visitors. As such, a CMS with the right kind of capabilities is now a strong tool to help meet GDPR requirements and to prove compliance. But remember: a CMS won't take care of all the privacy and data management work that the overall organization needs to do to comply with the GDPR.

First, to be useful for GDPR compliance, a CMS solution should already provide essential capabilities like:

- Digital marketing and marketing automation
- e–commerce
- Online forms
- Analytics
- Integration with other applications

Second, a CMS that has added capabilities that directly address ways to meet certain requirements of the GDPR, or is GDPR ready, will make it easier to comply with the rights of individuals regarding personal information. It can help demonstrate compliance with the data privacy and usage requirements when requested by individuals or regulatory entities.

Organizations gain more value from a CMS with GDPR–ready capabilities, rather than building everything using custom code. Coding everything from scratch can take a long time and can be error–prone and unwieldy for future changes and maintenance. On the other hand, a GDPR–ready CMS should offer certain options for custom code, since every organization will have somewhat unique needs for GDPR compliance.

Recommended GDPR–ready Capabilities Include

Tracking and Documenting Individual Instances of Consent

Every interaction between a visitor or customer and a web property or digital marketing activity (such as an email campaign) now involves separate consent. A GDPR–ready CMS provides integrated consent management capabilities to handle multiple consents specific to each interaction purpose and to bind them to the features and modules of the CMS. These capabilities should document: creation, storage, updating, or archiving of individual consent instances. The CMS should automatically recognize whether a visitor or customer provided consent for the current activity, and, if not, display the most recent version of consent with pertinent details.

Double opt–in validation models are important CMS mechanisms to ensure that the person giving consent is actually that person, which usually means sending a confirmation link to the email address for the person in question. When the person clicks on the confirmation link, consent can be considered valid. The double opt–in model must be repeated for each specific activity for that person.

Right to Access Personal Information and Consent

Individuals have the right to request copies of their personal information and consents from the organizations that are storing and/or handling such data. A GDPR–ready CMS provides access to such information through a single point or portal that makes it easier for organizations to quickly produce a compilation of personal data and deliver it in a timely manner, as required by the GDPR.

A CMS that stores the history of consent instances for each visitor also aids organizations in providing the information that visitors may want. A history of consent instances should include: data subject identifier; time stamp; the subject of the consent; how the consent was given (email, online form, etc.); if and when a consent instance was withdrawn.

Right to Be Forgotten

A GDPR–ready CMS includes a straightforward method to comply with requests from visitors for the deletion of personal information while meeting GDPR timeframes for completing the deletion. There are situations where not all personal information can be deleted, such as when certain information must be retained to comply with other legal requirements. The CMS should have mechanisms to identify what personal information must be retained.

The CMS should send notifications to all parties (whether controllers or processors) to let them know when they must delete personal information. The CMS maintains a log of notifications sent to separate parties, so that organizations can prove that notifications were sent.

A GDPR–ready CMS also provides a way for users to set up data retention policies for personal information in line with GDPR requirements.

Data Portability

People can request that an organization provide them with all of their information in a machine readable format to be exported to another system and/or organization. The GDPR–ready CMS includes capabilities to easily generate such data exports.

Data Flow Mapping

Organizations will need to map their data and information flows in order to make a proper assessment of their privacy risks under the GDPR. Simplifying accurate data mapping to locate specific data when requested is another beneficial capability for a CMS.

Governance and Workflow

A CMS with well–structured governance and workflows is practically indispensable for managing the extensive documentation requirements of the GDPR.

Reporting

CMS reporting capabilities play a key role for complying with customer rights to know more about how personal information is being handled. Reports should contain information such as: the purpose for processing customer data, categories of data subjects, what personal data has been processed, categories of third parties with whom data is shared, and data retention periods.

Custom Code Option

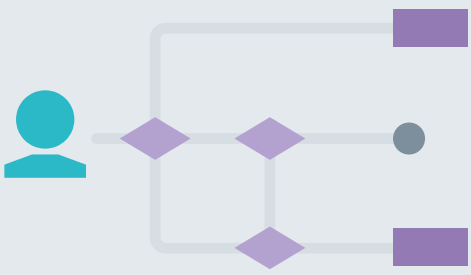
A CMS saves valuable time with many out–of–the–box capabilities. Often web developers need to be able to customize the sites that they are creating through custom code, to handle specialized needs. The same can be said of the GDPR–ready capabilities in a CMS, so it's helpful to provide a custom code option that is well–managed. Any custom code created in relation to GDPR compliance must be thoroughly documented and audit–ready.

Security Measures to Protect Information

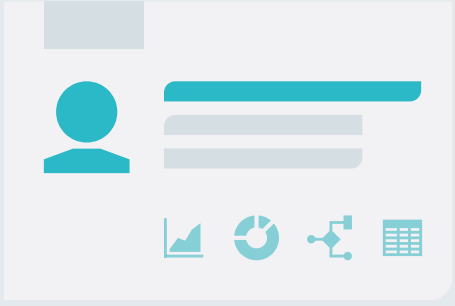
The intent of the GDPR is to maintain the privacy of personal identification information. To that end, CMS best practices and capabilities should include good security approaches to help protect visitor and customer data. It's best not to store personal information in a CMS. This kind of information should be stored in data management or CRM systems that have good privacy and security measures in place. Documentation should be created to outline specific measures related to CMS processing that can help protect customer information and privacy. CMS capabilities that ensure only authorized access to the CMS include user permission management that employs granular permission levels, sophisticated user authentication, and tracking for all website modifications and use of a full audit history.

Your CMS Should Be Your GDPR-Compliance Assistant, Not Your Nightmare!

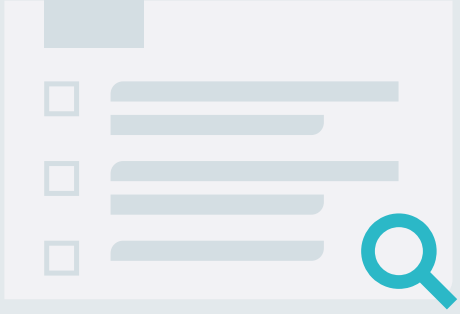
Because failing to meet the strict requirements of GDPR is punishable by painful fines, it is essential you plug a CMS into the heart of your tech stack that will help you avoid this. That is why Kentico 11's Data Protection app was designed with easier GDPR compliance built in. So when you need a solution you can trust, we've got you covered. We have prepared a typical GDPR compliance work flow to help explain this better. You must…



Map the data flow
Kentico 11 has mapped the data flow for you in its documentation

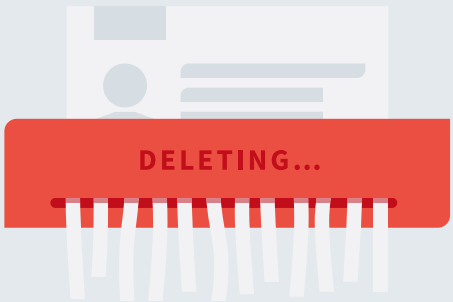


Organize an information audit
Kentico 11 speeds up the process by providing you with its mapped data flow

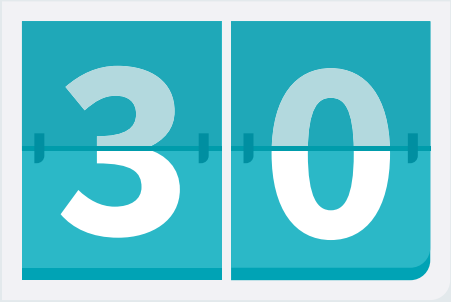


Review your current privacy notices
Kentico 11 makes it easier for you through integrated consent management

Check your procedures cover individuals' rights
Kentico 11 lets you manage individuals' rights with its Data Protection app

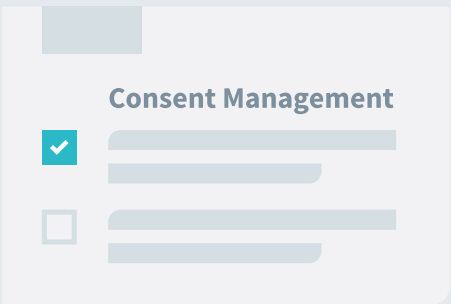


Be able to easily delete personal data or provide in usable electronic form
Kentico 11 allows you delete and access all data in its Data Protection app



Be able to fulfill any data request within 30 days
Kentico 11 improves your response time by letting you access all data via its Data Protection app

Review how you seek, record, and manage consents
Kentico 11 makes it straightforward with built–in consent management



Review existing consents so they meet GDPR standards
Kentico 11 helps you be more efficient through the Data Protection app

Your CMS doesn't do this?

Then time to change it. Kentico 11 gives you easier GDPR compliance, built in!

www.kentico.com