BetterCloud WHITEPAPER

Demystifying GDPR

IT's Crash Course to Compliance

Introduction

The General Data Protection Regulation (GDPR) is a complex regulation comprised of 99 articles. In this whitepaper, we'll break down the components of GDPR, clarify what they mean for IT, and list important action steps IT should take today. This content was written in partnership with Jodi Daniels (jodi@redcloveradvisors.com), a data privacy expert who has held senior privacy roles at Bank of America and Cox Automotive. She is the founder of Red Clover Advisors, a data privacy consultancy that assists companies with GDPR compliance, operationalizing privacy, digital governance, and online data strategy.

Part One will start with an overview of the regulation and why you need to start preparing now. Part Two will discuss some of the key elements including obtaining valid consent, access to data, and a data subject's right to be forgotten. Part Three will dive deeper into understanding the obligations of a data controller and data processor, as well as the newly defined role of a Data Protection Officer. Part Four will cover a ten-step checklist consisting of action steps that will help guide your GDPR compliance strategy. Finally, Part Five will explain in brief how BetterCloud can help with GDPR compliance.

May 25, 2018 is an important date for all companies who collect and store personal information on European Union (EU) citizens. It's the date that GDPR comes into force.

A common misconception is that this only applies to companies located in the EU. In the EU, privacy is a fundamental right. GDPR is applicable to all businesses that hold and process data collected in the EU, regardless if the company is located outside the EU. GDPR applies to you if you fall into one of these buckets:

- You are a company with US offices and have customers around the world
- You are a B2B company with US offices that serves EU clients
- You are a company with offices in the EU

GDPR sets a new high bar for how EU customers will expect their data to be treated by any company they interact with.

PART ONE

Overview: 11 Key GDPR Concepts You Need to Know

1. Data controllers & processors

GDPR affects both data controllers and data processors. The data controller defines how and why personal data is processed and determines the purposes for which the personal data is processed. Every company to some extent is a data controller, as at a minimum it's responsible for its employee data or those of its clients. The data controller is responsible for ensuring that the data processors are GDPR compliant. For the same data processing activity, a company must be either a data controller or a data processor.

Data processors are either internal groups or outsourced vendors that process personal data on behalf of the data controller. For example, if payroll is processed by a third party, then the payroll company is a data processor to your company. If you are a market research firm, you are a data processor to your clients.

Keep in mind, GDPR applies to both customer and employee data.

2. Data Protection Officer (DPO)

Companies may also need to appoint a Data Protection Officer (DPO) to oversee data security strategy and GDPR compliance. We will talk more about DPOs later in this whitepaper.

3. Noncompliance

Noncompliance with GDPR can be costly. Companies could face regulatory fines as high as four percent of their global annual turnover or €20 million, whichever is higher. GDPR is setting a new baseline for privacy and security, and EU customers will expect companies to comply. In addition to penalties, companies can suffer reputational harm from negative publicity about their noncompliance.

Supervisory authorities will have the ability to require documentation from companies or conduct audits. Data subjects will have the ability to submit a complaint to their local supervisory authority of either their residence, where they work, or where the data infringement allegedly happened. Data controllers and processors will also need to be prepared to present at court proceedings and adhere to any enforcement actions should that be required.

4. Personal data

GDPR expands the definition of personal data with special categories such as health, genetic, and biometric data. These special categories of data are deemed to be “particularly sensitive in relation to fundamental rights and freedoms” and as a result warrant special protection.

GDPR personal data elements include (but are not limited to) the following:

- Basic identity information such as name, address, and ID numbers
- Web data such as location, IP address, cookie data, and device identifiers
- Genetic data (e.g., an individual’s gene sequence)
- Biometric data (e.g., fingerprints, facial recognition, retinal scans, etc.)
- Racial or ethnic origin
- Political opinions
- Sexual orientation
- Religious beliefs

GDPR also introduces a new concept called “pseudonymous data.” This is defined as personal data that has been hashed or encrypted (or something comparable) with the intent that it cannot identify an individual without additional information. The goal is to separate the “personal” from personal data so that not all the parts to the puzzle exist in one place. Pseudonymous data with additional information could still be traced to the data subject and is considered personal data under GDPR.

Pseudonymous data would be ideal to use in data analytics and research. Since the personal data is not all combined, using pseudonymous data lowers the risk of misuse if exposed in a data breach.

5. Data processing

GDPR allows companies to store and process personal data only when the individual consents. Additionally, companies can store and process personal data for “no longer than is necessary for the purposes for which the personal data are processed.”

The cost to store data is historically low and many companies keep data longer than is necessary to conduct business. GDPR specifically states that companies should destroy data that is not needed to run daily operations, or use some type of encrypting, data mask, or comparable technology to protect the data. **Keep only the data required to do business.**

6. Cross-border data transfers

Transferring data outside of the EU is prohibited unless adequate protections are in place. Data transfers to a third country can be made if that country has been determined by the EU Commission to have adequate level of protection by decision (countries like Israel, Argentina, Canada, New Zealand, and Switzerland). For companies that have self-certified under Privacy Shield, data can be transferred to the US. Otherwise, adequacy can be met through safeguards such as Standard Contractual Clauses or Binding Corporate Rules (BCRs). In short, BCRs are EU-approved (under the EU cooperation procedure) internal rules adopted by multinational companies to make intra-company transfers of personal data.

7. Right to be forgotten

GDPR introduces the concept of the right to be forgotten, which allows a person to request their data to be erased. There are some exceptions (for example, it cannot supersede any legal requirement that an organization maintain certain data). For US companies, this would include HIPAA required records.

8. Data portability rights

Data subjects can demand their personal data be ported to them so they can reuse “their” data for their own purposes and across different services. This applies to online data only. Data controllers need to provide functionality that enables the data subject to move, copy, or transfer personal data easily. Examples could include a list of media such as books, songs, movies, photos stored in a cloud, or transaction history. Data that is inferred such as behavioral data determined from analysis would be out of scope.

9. Report a breach within 72 hours

If your company experiences a data breach, you must notify the local Data Protection Authorities (DPA) in the member states of those affected within 72 hours of identifying or confirming the occurrence of a data breach. Companies need to prepare with a rehearsed incident response plan comprised of a cross-functional team including public relations, legal, compliance, IT, privacy, and information security professionals.

10. Processing of data requires consent or legitimate interest

Under GDPR, the use of data must be via opt-in consent or meets the definition of legitimate interest. This is opposite many US regulations where only providing opt-out is required. Consent must be documented, separate from other terms and conditions, cannot include pre-checked boxes, must specifically state the use case of the data being processed, and list any third parties that will also rely on this consent. Additionally, the user must be able to withdraw the consent.

11. Accountability

GDPR significantly impacts how companies collect, store, and transfer personal data. Companies must not only comply, but also be able to demonstrate compliance. There must be a privacy impact assessment program in place to review any data processing activities that would cause a “high risk to rights and freedoms” of a data subject.

Don’t delay—start planning now!

Companies need ample time to prepare for GDPR. This includes performing assessments, documenting the data flow in a company, and remediating any gaps identified during the process.

Get started now on crafting a plan, securing resources and budget, and determining any assistance you will need from external legal counsel and consultants. Ensure your company has adequate time to manage any project delays or unexpected findings, and to implement any new controls or processes to ensure GDPR compliance.

Companies not in compliance by May 25, 2018 risk hefty fines, scrutiny by local supervisory authorities, and negative PR. There is also the potential loss of customers as companies need to ensure they work with GDPR compliant vendors.

GDPR readiness is not a one and done activity. Compliance will need to be reviewed annually. As a part of the GDPR readiness activities, processes to ensure ongoing compliance with GDPR should be considered. Examples include:

- Updating contracts with appropriate GDPR clauses
- Updating data inventories with changes to personal data collected, used, or stored
- Reviewing and updating external privacy notices and internal policies
- Building into the product plans consent capture, data portability, and right to be forgotten

Preparing for GDPR compliance ahead of time can help companies get a clear picture on their data activities, such as knowing what personal data is collected, where it is stored, and how it is used. Customers expect that you take privacy and security seriously. For GDPR compliant companies, it will ultimately help keep data safer.

Knowing where all your data is stored will help your company be more agile and efficient, which translates into better decisions. As companies are looking to partner with GDPR-compliant organizations, being ahead of the curve as an early adopter can help you stand out amongst the competition.

PART TWO

The Right to Be Forgotten, Obtaining Consent, and the Right to Data Portability

Here in Part Two we will discuss some of the key elements of GDPR in more detail, including the right to be forgotten, obtaining valid consent, and the right to data portability.

The right to be forgotten

Users can request their data be erased

GDPR introduces the concept of the right to be forgotten, which allows a person to request that their data be erased. This applies to all data controllers. (Every company to some extent is a data controller.)

According to Article 17, data controllers must erase personal data "without undue delay" if the processing was unlawful, the data is no longer needed, or the data subject objects to the processing. In GDPR lingo, the data subject is the person whose data has been collected, aka "the user or the customer."

There are some exceptions (for example, it cannot supersede any law requiring an organization to maintain certain data. For US companies, this would include HIPAA-required records).

This requirement extends to any company that has made personal data public, especially if it's online (e.g., an online forum or social media community). The data controller is required to take "reasonable steps," defined as cost to comply and technology available, to inform any other controller who has processed the data about the data subject's request.

Important steps IT should take now

1. Perform a data inventory so it is clear where a data subject's data resides.
2. Determine if data erasure requests would be unreasonable or unwarranted, or if any exemptions are required, in your company's industry. For example, there are certain retention requirements around financial or health data. Also determine if your systems need any work done in order to flag data as restricted while a complaint is being processed. If there is data that cannot be erased (e.g., bank records that have to be maintained per legal requirements for a period of time), then your systems need to be configured so that these fields can be appropriately marked as not to be deleted.
3. Design a process that will manage data erasure requests.
4. Provide training for employees on how to identify and handle data erasure requests.

Obtaining valid consent

Processing of data requires consent (or legitimate interest)

The concept of data processing is a key element under GDPR. Data processing can include everything from using an employee's data to process payroll, using a customer's information to send marketing emails or targeted advertising, or serving as a SaaS provider.

Under GDPR, the way users consent to data processing is either by opting in or meeting the definition of legitimate interest. Under the current European Data Protection Act (DPA), consent has been a foundation of privacy law. However, GDPR increases the requirements significantly.

Article 6.1 of the GDPR defines the lawful grounds for data processing as summarized below:

- Consent has been given for a specific purpose
- To deliver on a current contract, or just before entering into one
- Due to a legal obligation
- To protect the vital interests of the data subject or another person
- If acting in the public interest or required by a public authority
- For purposes of legitimate interests (note that there are some exceptions like if a child is involved)

"Say what you do, and do what you say"

Under GDPR, companies must be very transparent about what they're doing with users' data. The notion of "say what you do and do what you say" is evident in the GDPR consent requirements. Here are six points to keep in mind:

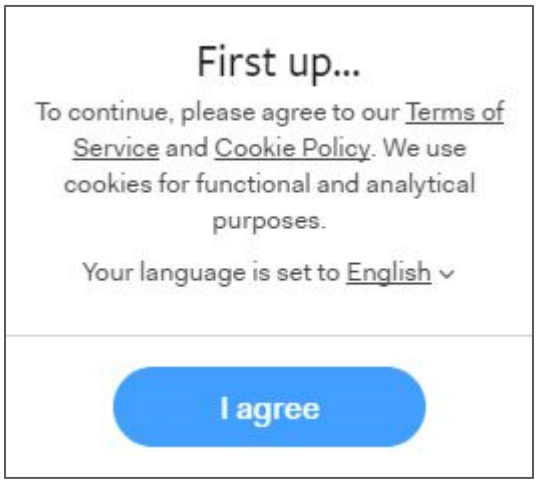
1. Consent must be freely given. Consent should be separate from terms and conditions and should not be a condition to signing up for a service unless it is required for that service.
2. Consent must be easy to understand and specific for each use. The company may only use the consent for that specified purpose.
3. Consent needs to be granular and broken down by type, such as advertising or analytics.
4. The user must specifically opt in. There can be no use of pre-checked boxes.
5. Companies need to retain proof of consent including what the user has consented to, what the user was told at the time, and what the method of consent was.
6. Users should be able to easily withdraw consent.

New cookie policies

Today, it is common for companies to engage in informed consent by displaying a banner on their website, telling the user that tracking cookies are being used.

Here's an example:

In some cases, the user has the option to learn more and must press "accept" or "I agree" in order to continue to the site. Under GDPR, cookie policies can no longer prevent users from accessing content.



European data protection authorities in the UK, France, and Germany state that consumers must be told in a clearly written notice before tracking cookies are used. **The user must opt in by checking a box on a website. Obtaining consent in this manner will require software engineers to build this requirement into the design.**

With the complexities of the online advertising ecosystem, it is critical to understand which vendors are on the site collecting data. **Now more than ever, companies need to have a digital governance process.** This includes having contracts with their agencies and marketing partners, as well as performing regular monitoring of the site.

Tag management platforms will catch which tags have been placed on the site. They will not always show the daisy chain effect of tags and cookies. For each tag that fires on the site, the company is responsible for any data that is collected on the data subject. Malware can also exist through an ad tag, allowing hackers to take down a website, steal data, or redirect users when they click on an ad. All of this increases the risk of a data breach.

Marketing & IT must work together to prove consent

The ability to prove consent is a requirement of GDPR. **Marketing and IT departments will need to work closely together to ensure that consent is captured, stored, and readily available.** It will also be important to know what version of the privacy notice was provided at the time consent was given. For example, if a user provides consent on June 1st and the privacy notice is updated on July 15th, the company needs to know what was included in the privacy notice on June 1st, since that was the date consent was given.

The right to data portability

GDPR puts data rights in the hands of data subjects

GDPR introduces the concept of data portability. This means that data subjects can demand their personal data be ported to them if they provided their data to the controller, provided consent to the controller, or were engaged in a contract whereby the controller was using their data and processing of the data was automated.

Data subjects will have the right to port their data and reuse "their" data for their own purposes and across different services. This applies to online data only.

Data controllers need to provide functionality that enables the data subject to move, copy, or transfer personal data easily. The data must be provided by the data controllers in a commonly used and "machine-readable" format. There is no specification on how companies should make this data available.

Companies need to make it easy to export data

Given how GDPR puts privacy rights in the hands of data subjects, companies should make it simple for the data subject to port the data. For example, companies could offer a simple self-service tool for data subjects to use. It should allow the data subject to determine which fields can be exported and should also consider the security of how the data is exported. Data subjects can then transmit that data to any other data controller. In some situations, the data controller might be required to send the data directly to a competitor.

Examples of data could include a list of media such as books, songs, movies, photos stored in the cloud, or transaction history. Data that is inferred, such as behavioral data determined from analysis, would be out of scope.

IT's roles and responsibilities

To adhere to the consent, right to be erased, and right to port data clauses under GDPR, it's critical for companies to understand what data they have, where it is stored, and how it is being used. This is where IT can play an extremely valuable role. Companies then need to create processes to manage consent, the right to be erased, and the right to port data. And finally, companies must also train employees on these new requirements and processes.

PART THREE

Data Controllers vs. Data Processors, Reporting Data Breaches in 72 Hours, and Data Protection Officers

Data controller vs. data processor: Which one are you?

The basic definition

Let's begin by understanding the difference between the controller and the processor. It's important to know which one you are, since the obligations under GDPR can differ for each.

Officially speaking:

Controller – "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data…" Basically, the controller makes the decisions about the data. This can mean employee, customer, or vendor data. Every company to some extent is a data controller; at a minimum it's responsible for its employee data or those of its clients.

Processor – "The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Basically, the processor receives instructions from the controller on how to process the data. Cloud service providers and payroll companies, for example, are processors. A data processor is directly accountable to those whose data they process.

Sometimes companies can find themselves in a joint-controller situation, where two or more data controllers determine the purposes and means of processing of personal data. Companies also can be both a controller (for its employee, customer, and vendor data) and a processor (for its main line of business).

What does a data controller need to do?

Be very transparent

Companies need to disclose how they use personal data, how long they store it, the use of third parties, etc. This is normally done in a privacy notice. Keep in mind that a privacy notice needs to be provided to all individuals whom personal data is collected from. This includes employees, vendors, customers, and consumers.

Report data breaches within 72 hours

So what constitutes a data breach under GDPR? A “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.” This is beyond just the risk of fraud or identity theft common in the US data breach laws.

Controllers are responsible for reporting a data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it. Processors are responsible for reporting a data breach without undue delay to data controllers after becoming aware of it. There is a close-knit relationship between controllers and processors.

There are a few reporting exceptions. One is if “the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons.” With no guidance or case law yet, it will take some time to fully comprehend what will result in a risk to the rights and freedoms of a person and what will not. It is advisable to err on the side of conservativeness.

Select processors and sub-processors

Data controllers must select data processors that can provide sufficient guarantees that it has technical and organizational measures in place to meet requirements under GDPR. Processors must process personal data per the controller’s instructions. This means that processors have to comply with many of GDPR’s requirements, per the controller’s instructions.

The data processor can also use sub-processors with the controller’s specific or general written consent. This consent can be obtained at the beginning of the contract. Companies should review all their contracts with third parties that process data on their behalf to ensure compliance. They need to make sure both parties’ obligations and responsibilities under GDPR are clearly defined.

Honor new privacy rights for individuals

GDPR creates new individual privacy rights, like the right to be forgotten and the right to data portability. The controller must be able to meet the requirements for these new rights.

A data subject has the right to go to a data controller and request their data be deleted (aka the right to be forgotten) or made available to them (aka the right to data portability). Then, the controller will inform its data processors (which could be you if you are a data processor) what information needs to be deleted or made available to the data subject.

Controllers and processors will need to thoroughly vet this process and determine how requests will be managed. Once determined, this should be covered in the written agreement.

Create contracts between data processors and data controllers

Data controllers and data processors will need to specifically outline the requirements and responsibilities in their contract. The contract should cover the term, the nature and purpose of processing, the types of data to be processed, as well as the obligations and rights of the controller.

Additionally, the contract needs to specifically address that data should only be processed at the direction of the controller, that the data processor will need to report any breaches to the data controller without undue delay, and finally, how the data processor may need to assist the data controller to fulfill individual rights obligations under GDPR (such as the right to erasure or data portability).

A new role: Meet the Data Protection Officer (DPO)

Do you need to appoint a DPO?

Well, it depends. Under GDPR, companies will need a DPO if it is processing personal data that requires "regular and systematic monitoring of data subjects on a large scale" or where the core activities of the processing involve large amounts of sensitive data. Examples include companies that must process health records to serve its patients, or engage in online tracking and profiling (like email retargeting, location tracking, or processing customer data at a bank).

There are some exceptions for companies who have fewer than 250 employees. However, it is dependent on the types of data being processed. Appointing a DPO applies to both data controllers and data processors.

What does a DPO do?

The DPO is the company's main point of contact to a supervisory authority as well for any data subjects. The contact details for the DPO need to be published (often in a privacy notice) and communicated to the supervisory authority.

Additionally, the DPO's role is to inform the company about its obligations under GDPR, monitor compliance, and advise on privacy impact assessments. While it is not specified, the DPO should have knowledge in data protection law and practices. A DPO can be an existing employee or a contractor. The DPO should report to the highest level of management (including the board of directors) but will work independently.

PART FOUR

What to Do Next: A 10-Step Checklist

Now that you have an understanding of the fundamentals of GDPR, what should you do next? Here is a 10-step checklist to get you jump-started on your path to compliance.

1. Designate a GDPR resource in the company who will lead the project. Consider outsourcing for additional help.

2. Know what data you collect, hold, share and store including cloud applications that are processing or storing your data. This likely involves performing a data inventory.

Remember: GDPR is bigger than just personally identifiable information (PII). Personal data under GDPR includes online identifiers like cookies, location data, and sensitive data like race, political views, and biometric data. This is just a short list!

3. Collect only necessary data.

4. Limit processing of "sensitive" data such as race, ethnicity, political views, religion (reminder: all of these need consent).

5. Review and update agreements with all data processors and third parties (where applicable).

6. Conduct or respond to inspections and audits of data processors either directly or through an external auditor to ensure compliance.

7. Make sure processors only use personal data for the designated purpose. If you are a processor, make sure you process data only for purposes you have agreed upon in the contract and for which consent was provided.

8. If you work with a sub-processor, make sure that you have the appropriate agreements and notices in place to do so.

9. Ensure security measures are in place for both data controllers and processors to protect personal data from loss or unauthorized processing. Here are some essential points to review:

- Does the vendor have a well defined and clear access control policy?
- Who can access your company's data and when? Is this access tracked?
- Does the vendor have a designated person responsible for security and data protection?
- How does the vendor secure data?
- What is the company's data retention policy?
- For data that is to be deleted, you need to ensure that data is not copied and located in multiple places, and that there are mechanisms in place to evaluate that the data has been deleted when required.

10. At the end of the service term and if requested by the controller, the processor must delete or return all the personal data to the controller relating to the processing. It must also delete all existing copies (unless the EU or the Member State law requires storage of the personal data). Processors can request an inspection to ensure that this has been done.

PART FIVE

Leveraging BetterCloud for GDPR

GDPR REQUIRES YOU TO:	BETTERCLOUD ALLOWS YOU TO:
Control Access to Personal Data A pillar of GDPR is limiting who has access to crucial data in your domain. While it sounds simple, consolidating a list of administrators is tricky. Limiting and tracking access to your applications can prove even trickier.	**Enforce a Least Privilege Model** Restrict who can view, create, edit, and delete your most sensitive data objects using privileges based on job requirements Consolidate permission controls for your critical SaaS applications in one view
Follow The Right to Be Forgotten This rule allows a person to request that any data a company owns about them be deleted. This can be anything about a specific individual, ranging from a social security number to a CRM record. While this rule cannot supercede another law (like a requirement to maintain HIPAA records), it is essential for any company who houses personal data online.	**Discover and Delete Data** Uncover files containing personal data by performing a Google Drive audit in BetterCloud Remove ex-employee data from SaaS applications using automated workflows Ensure correct actions have been taken to delete data through comprehensive audit logs and workflow results
Report a Breach in 72 Hours In the case of a personal data breach, the controller needs to notify their local Data Protection Authority figure within 72 hours after becoming aware of it. Companies should have a cross-functional incident response plan prepared that includes the Public Relations, Legal, Compliance, IT, and Security teams.	**Deploy Advanced Alerts & Policies** Notify teams about potential threats in your environment through advanced alerts with custom escalation paths Remediate dangerous situations immediately and prevent future breaches using automated Policies Discover potential causes of a breach by reviewing admin actions in audit logs
Comply with Data Portability Similar to the Right to Be Forgotten, Data Portability requires companies to surface all the data they have about a person. Instead of simply deleting these records, companies must send the data to the person, if they request it.	**Centralize and Locate Data** Detect files containing personal data by running a Google Drive audit in BetterCloud Centralize files into a single folder containing all of an individual's data to easily share with them

Want to learn more about leveraging BetterCloud to comply with GDPR?
Get in touch at bettercloud.com/gdpr

Demo BetterCloud today

About BetterCloud

BetterCloud is the first SaaS Application Management and Security Platform, enabling IT to centralize, orchestrate, and operationalize day-to-day administration and control for SaaS applications. Every day, thousands of customers rely on BetterCloud to centralize data and controls, surface operational intelligence, enforce complex security policies, and delegate custom administrator privileges across SaaS applications. BetterCloud is headquartered in New York City with an engineering office in Atlanta, GA. For more information, please visit **www.bettercloud.com**.