Tackling GDPR Compliance and the Right To Be Forgotten

A Privacera Use Case
May 2021

Content

1 Executive Summary

For organizations that collect, process, and store personal data of citizens of the European Union, achieving and maintaining compliance with the General Data Protection Regulation (GDPR) is not optional. Failing to do so has the potential not only to impact an organization's business reputation and incur hefty fines, but also, in extreme cases, to threaten its ability for continued operations.

This paper takes a look at the current GDPR landscape, while explaining the roles and responsibilities of associated parties. Particular attention is paid to a key requirement demanding the attention of today's data privacy, security, and compliance officers: the Right To Be Forgotten (RTBF). We subsequently introduce the Privacera multi-cloud data security and access governance platform and highlight the ways it can help today's businesses achieve and maintain compliance with the GDPR, both in general and is it relates to the RTBF.

2 GDPR Fundamentals

Organizations of all types and sizes worldwide must contend with an array of data privacy and protection regulations that impact numerous aspects of their operations.

For entities operating in the U.S, there are the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX), as well as state laws like the California Consumer Privacy Act (CCPA). Merchants worldwide that handle credit and debit card data must also comply with the Payment Card Industry Data Security Standard (PCI-DSS).

However, for organizations in Europe — or that handle the data of EU residents — the chief concern these days is the GDPR. The regulation specifies how firms process, protect, and notify individuals living in the EU regarding their personal data, including all aspects of collecting, storing, transferring, or using that data.

GDPR's Global Impact

While GDPR regulates personal data of EU residents, it can affect any organization, regardless of location.

If an organization is not located in the EU but handles personal data on EU residents, it is still subject to GDPR requirements. For example, if an organization is not in the EU but has EU customers, it is subject to GDPR. If an organization uses web tools that allow it to track cookies or the IP addresses of people who visit its website from EU countries, it is subject to GDPR.

Organizations that handle personal data are defined as “data controllers,” and third parties that process data on behalf of data controllers, such as email service providers, are called “data processors.”

In particular, GDPR lays out seven protection and accountability principles for data controllers and processors to follow:

Lawfulness, fairness, and transparency: Data processing needs to be lawful, fair, and transparent to the data subject.

Purpose limitation: Data can only be processed for the legitimate purposes specified explicitly to the data subject when it is collected.

Data minimization: Only as much data as necessary for the purposes specified can be collected and processed.

Accuracy: Personal data needs to be kept up to date and accurate.

Storage limitation: Personal data can only be stored for as long as necessary for the specified purpose.

Integrity and confidentiality: Data processing must be performed in such a way as to ensure appropriate security, integrity, and confidentiality.

Accountability: Data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

The GDPR mandates that firms have policies and procedures in place to ensure the security of personal data. Further, firms are required to conduct impact assessments to validate that data security and privacy are being maintained.

Organizations need to create and implement policies and processes to ensure data security, integrity, and availability. Recommended data security measures include encryption, endpoint security, and pseudonymization.

Some, but not all, organizations must appoint a data protection officer (DPO), especially if a firm is performing large-scale systematic profiling and monitoring of individuals.

Under GDPR, organizations need to report data breaches to data protection regulators and to affected individuals within 72 hours in most cases. They must also record when a breach occurred and identify the data that was accessed or altered.

It is important to note, too, that GDPR provides for remedies, liabilities, and penalties for violations. There are two tiers of fines for GDPR violations. Less severe violations could result in a fine of up to €10 million, or 2% of an organization's worldwide revenue, whichever is greater. More severe violations can result in penalties up to €20 million or 4% of a company's annual global revenue, whichever is greater.

Nothing to Sneeze At

As of March 2021, EU regulators have levied more than €270 million in 569 fines for GDPR violations. Some of the levies have exceeded €20 million, such as France's €50 million fine on Google, Germany's €35 million fine on H&M Hennes & Mauritz Online, Italy's €27.8 million fine on TIM, and the U.K.'s €22 million fine on British Airways.

3 GDPR — For The People

Overall, GDPR reflects the fact that individuals are trusting organizations with detailed information about their personal lives — such as email addresses, location, ethnicity, gender, biometric data, religious beliefs, web cookies, and even political opinions — that must be protected.

As a result, it is not surprising that the regulation, at least to some extent, puts customers and constituents in charge of how their personal data is handled.

In particular, GDPR grants specific rights to people whose data is being processed, known as "data subjects."

- **Right To Be Informed.** Data subjects have the right to know what data has been collected about them, the reason for the collection, and how the data is being processed.
- **Right Of Access.** Data subjects have the right to access personal data that is being processed and to request copies of personal data.
- **Right To Rectification.** Data subjects have the right to modify data they consider inaccurate or out of date.
- **Right To Erasure (aka, Right To Be Forgotten).** Data subjects have the right to have their data deleted under certain circumstances.
- **Right To Restrict Processing.** Data subjects have the right to request that their data be marked as "restricted" and not be accessed or processed without permission.
- **Right To Data Portability.** Data subjects have the right to request a transfer of their personal data to another organization.
- **Right To Object.** Data subjects have the right to protest the processing of their personal data in certain circumstances, such as regarding a legal dispute.
- **Rights Concerning Automated Decision Making And Profiling.** Data subjects have the right to object to the automated processing of their data for profiling, loan application decisions, or other actions.

Key GDPR Requirements Organizations Need to Address

Data breach
Organizations have 72 hours to report breaches involving personal data

Guaranteed data portability
Data subjects can request to have their data transferred to a third party

Right to be forgotten
Data subjects can request organizations to delete their personal data

4 Details of The Right to be Forgotten

Although all of the “rights” of data subjects are clearly important, the RTBF can be especially challenging for data privacy and compliance teams to address. The presence of similar requirements in other global regulations — such as Brazil’s General Law for the Protection of Personal Data (LGPD) — further warrants us taking a closer look at this one in particular.

To begin with, it is important to understand that a data owner can make a request to delete their personal data, verbally or in writing, to any member of an organization, not just a designated contact. Digging deeper, the regulation states that “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 an obligation to erase personal data without undue delay where one of the following grounds applies:

- The personal data is no longer needed for the purposes for which it was originally collected or processed.
- The data subject withdraws consent on which the processing is based and where there are no other legal grounds for processing.
- The data subject objects to the processing, and there are no overriding legitimate grounds for the processing.
- The personal data was unlawfully processed.
- The personal data must be deleted to comply with a legal ruling or obligation.
- The personal data was collected concerning the offer of information society services to a child.”

It also goes on to identify scenarios where the organization's right to process personal data overrides the individual's right to be forgotten, including when:

- The data is being used to exercise the right of freedom of expression and information.
- The data is being used to comply with a legal ruling or obligation or perform a task that is being carried out in the public interest or the exercise of the controller's official duty.
- The data being processed is necessary for public health purposes and serves the public interest.
- The data is being processed for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.
- The data is being used to establish a legal defense or in the exercise of other legal claims.

On top of everything else, an organization can require a "reasonable fee" or decide not to delete data if it can show that the request was unfounded or excessive.

The bottom line is that there are many variables at play, and an organization will have to evaluate each request on its individual merits. What's clear, however, is that organization must have the technical means not only for keeping track of ALL locations where a data subject's personal data is stored, but also for expunging that data, or otherwise making it, inaccessible to unauthorized parties or systems.

5 Getting Started with GDPR Compliance

For organizations that lack a structured approach, achieving and maintaining GDPR compliance can be an overwhelming endeavor. Data privacy risks must be balanced with the values of business strategies and operations. To prioritize their initiatives, organizations should focus first on high-risk and high-value areas of their ongoing operations.

As part of their overall risk assessment framework, organizations should set up processes to determine who owns specific regulatory risks and to define escalation procedures when encountered risks exceed thresholds the business is willing to accept.

Developing a corporate “risk and privacy culture” is also an important step in the overall process, including establishing programs to educate not just management teams but also rank-and-file employees on both GDPR in general, as well as the specific ways the regulation intersects with each of their jobs.

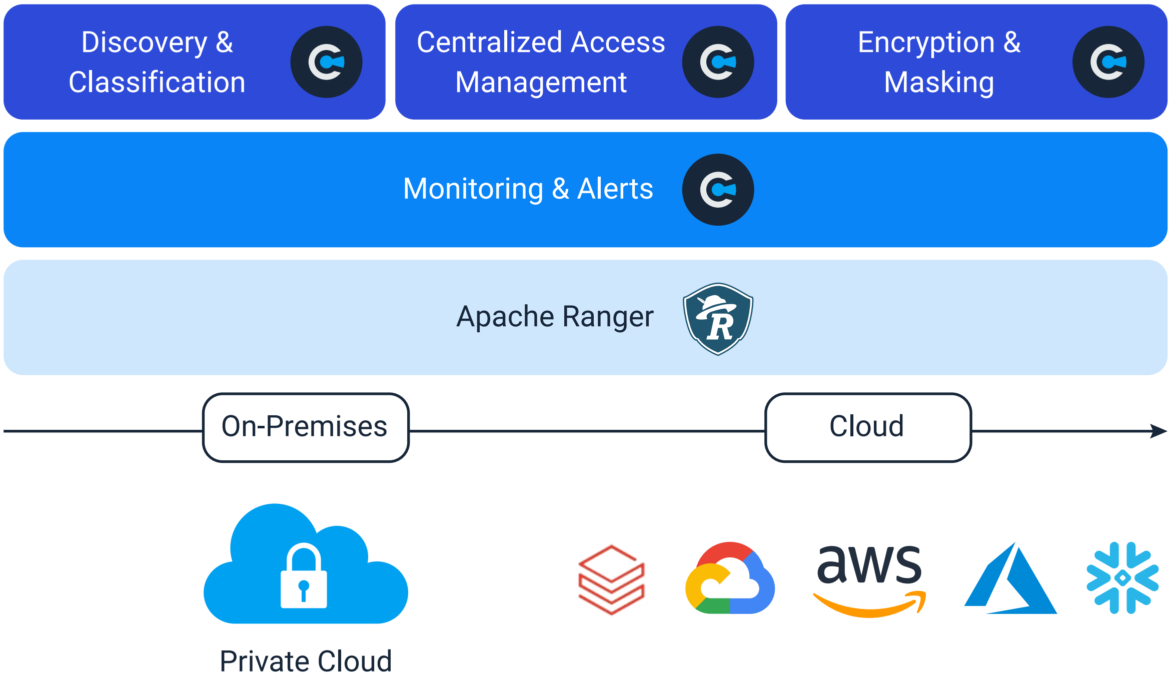
From a technical perspective, IT teams must then turn to implementing processes and technology solutions that enable them to effectively and efficiently:

1. Identify personal/sensitive data within ALL of the organization’s repositories
2. Classify personal/sensitive data by applying tags
3. Build access control policies using roles, attributes, and tags
4. Mask and encrypt personal/sensitive data, as appropriate
5. Perform regular audits to determine the effectiveness of the access control policies (and other measures)

6 How Privacera Supports GDPR Compliance

Privacera provides a centralized data security and governance platform that can be deployed in both SaaS and a customer's own AWS, Azure, or Google Cloud environment. The platform enables analytics teams to access and utilize all types of data in all locations while ensuring data security, privacy, and compliance requirements are met. An Apache Ranger-based architecture enables scalability to petabytes of data.

The Privacera Platform



Automated data discovery helps customers get visibility into sensitive or personally identifiable elements in their data. A combination of keyword dictionaries, patterns, advanced algorithms, and data science models can be used to identify and classify sensitive data and provide visibility across data platforms located both in the cloud and on-premises.

The platform eliminates manual processes by automatically detecting, cataloging, and otherwise processing sensitive data as it is ingested. The result is the ability both to assess and help ensure compliance with not only GDPR, but also Brazil's LGPD, PCI DSS, HIPAA, CCPA, and the recently enacted Virginia Consumer Data Protection Act, which contains many of the same provisions as the CCPA.

Centralized access control is enabled by single-pane-of-glass administration and auditing of data access policies. The platform provides federated authorization across multiple systems and seamlessly applies policies across various cloud services in all major cloud platforms (AWS, Azure, and Google Cloud).

The result from a compliance perspective is consistent data usage and sharing across multiple cloud databases, analytics platforms, reporting systems, and geographies. The platform is architected for cloud scale and performance, and delivers dynamic access control based on roles, data, and metadata.

Automated compliance workflows enable IT teams to use and share data, while easily adhering to applicable privacy constraints.

Privacera Compliance Workflows enable data owners to create data zones based on domains, business functions, or other logical groupings and apply customized policies across the data zone. Data zones simplify data access management and relieve IT of the burden of managing policies for the entire enterprise.

Enterprise-grade encryption and related features enable organizations to leverage regulated data for essential business processes while still maintaining the highest levels of privacy and confidentiality. With the Privacera Platform, sensitive data can be encrypted, while other elements remain free and clear for use by data scientists, analysts, and other users that have a legitimate business need to see and/or use it.

The Privacera Platform supports Advanced Encryption Standard (AES) and format-preserving algorithms. It can leverage open-source technology, including Apache Ranger's Key Management Service, and store and manage encryption keys for cloud services. It also integrates with external HSMs and key vaults, providing a high-security option for storage of related encryption keys.

Customers using PrivaceraCloud, the industry's first SaaS-based governance solution can take advantage of the above-mentioned capabilities as a fully managed service, without the burden of their IT having teams to install or manage the platform.

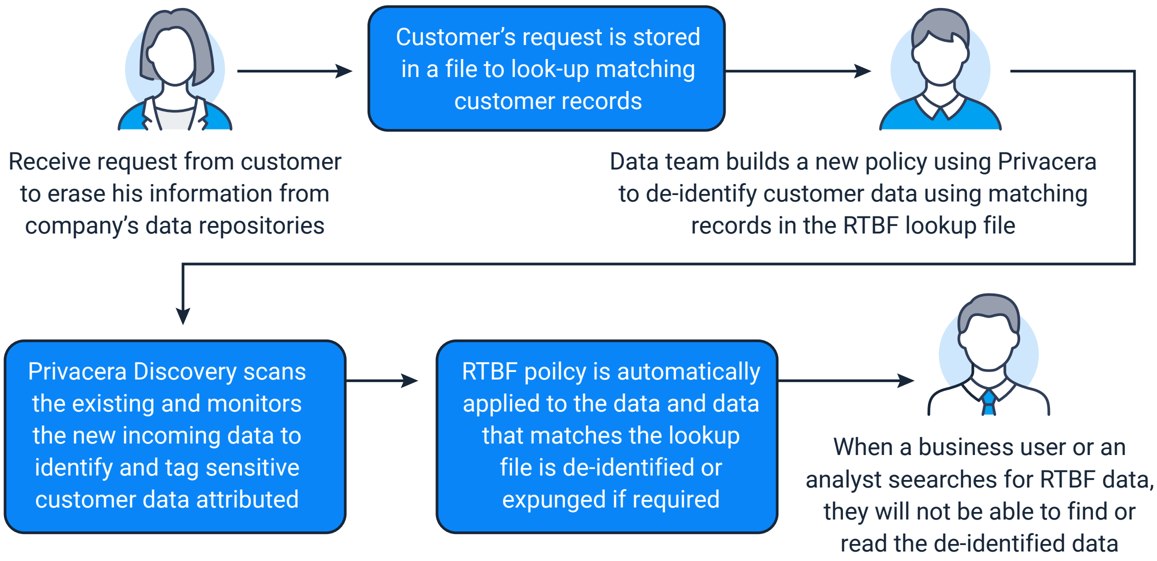
7 Privacera Compliance Workflows for Right to be Forgotten

In addition to the broad support its automated data discovery, centralized access control, and granular encryption capabilities provide for complying with GDPR and other data privacy regulations, the Privacera Platform, with its automated Compliance Workflows, also streamlines processes needed to address associated RTBF and right to access data requirements. Customers can reduce, if not eliminate, the otherwise manual and piecemeal processes required to establish and maintain compliance with these and other "rights" of data subjects. Let's look at an example to see how this works.

It goes without saying that you already collect customer data for a variety of purposes and store it in multiple formats and locations. You then receive requests from customers who want their data deleted. These requests are stored in a file which is used by the Privacera Platform to look up matching customer records in data stores where the personal data needs to be deleted. A data team member then sets up a new policy that de-identifies customer data using matching records in the look-up file. Privacera scans for and applies the new policy to matching data, such as email addresses, phone numbers, Social Security Numbers, addresses, and other regulated data. The whole process is automated end-to-end.

If someone at the company subsequently searches for this data, they will not be able to find or read it. As a result, your organization is compliant with the RTBF requirement. If desired, another compliance workflow can be configured to expunge the de-identified data, whereby it is permanently removed from the organization's data stores.

RTBF Compliance Workflow



Receive request from customer to erase his information from company's data repositories

Customer's request is stored in a file to look-up matching customer records

Data team builds a new policy using Privacera to de-identify customer data using matching records in the RTBF lookup file

Privacera Discovery scans the existing and monitors the new incoming data to identify and tag sensitive customer data attributed

RTBF poilcy is automatically applied to the data and data that matches the lookup file is de-identified or expunged if required

When a business user or an analyst seearches for RTBF data, they will not be able to find or read the de-identified data

8 Privacera Data Zones

A central aspect of the Privacera Platform is the data zone, which is a logical group of data across different data domains. The data zone can be created based on department, function, or a specific purpose — such as to manage the requests received from customers to expunge their data. For example, a data zone can be created to manage customer data under the management of a data administrator from the finance organization. Data zones enable data owners and stewards to create and maintain policies to ensure compliance for all of the data they manage.

Data zones also enable policies that allow authorized users to run analytics on decrypted data, while for all other users the same data remains encrypted. Similarly, authorized users from a supported application can access the decrypted data, while access is denied to unauthorized users.

Privacera's ability to customize what data to encrypt at the attribute level has several important applications. Now companies have the flexibility to encrypt only sensitive data, such as right-to-be-forgotten data, in a file or database. This targeted encryption allows companies to conduct advanced data analytics without compromising data security, or the privacy requirements of regulations such as GDPR, PCI-DSS, HIPAA, and so forth.

Data zone and attribute level encryption can also be combined with transparent data encryption (TDE), which encrypts all data on a disk, for a comprehensive data encryption strategy for any organization.

9 Conclusion

Privacera is used and trusted by Fortune 500 companies to manage and secure their sensitive data assets. We help customers meet data protection regulations like GDPR, CCPA, HIPAA, PCI-DSS, and others.

We enable customers to access the data they need while meeting stringent data privacy rules, such as GDPR's right to be forgotten. And we do it from a simple single pane of glass that provides data visibility, governance, and security across multiple cloud platforms.

To find out what we can do for you, visit our website today.