SOLUTION BRIEF
EU GDPR

GDPR Compliance: How Can You Adapt to the New Regulation?

ca technologies

Companies have complied with data protection directives and regulations for more than two decades. But the General Data Protection Regulation (GDPR), an overhaul of existing European Commission data protection legislation, aims to strengthen and unify those laws for EU citizens. Primary GDPR objectives are to give citizens back control over their personal data, and simplify the regulatory environment for international business. For organizations already compliant with Directive 95/46/EC, what do they need to do from a technology perspective to comply with GDPR?

Section 1:

Introduction to GDPR

By 25 May 2018, any organization that processes personal data of EU citizens needs to be compliant with GDPR. This regulation introduces new data protection requirements that will impact the majority of businesses across all sectors. Organizations that fail to comply with GDPR may face administrative fines up to €20,000,000 or up to 4 percent of global turnover, whichever is higher.

While GDPR has raised the bar in terms of data protection, it also seeks to harmonize the privacy laws across the European Union (EU), which should, to some extent, help businesses adopt more standardized data protection policies and processes.

The table below categorizes the GDPR requirements at a high level:

Category	Requirements
Rights of data subjects	1. Data subjects (see definitions 1) have the right to: a. Access their data. b. Rectification, erasure (right to be forgotten) and restriction of processing (see definitions 2). c. Data portability. d. Object to the use of their data.
Accountability	2. Those processing personal data are obligated to: a. Implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR. b. Obtain consent from the data subject for certain processing activities. c. Implement appropriate data protection policies and processes. d. Maintain a record of processing activities. e. Notify certain personal data breaches to the supervisory authority. f. Notify the data subject of certain personal data breaches. g. Designate a data protection officer where appropriate.
Data protection by design and by default	3. Implement appropriate technical and organizational measures that: a. Are designed to implement data protection principles, such as data minimization and pseudonymisation, in an effective manner and to integrate necessary safeguards of processing. b. By default, do not make personal data accessible without the individual's intervention to an indefinite number of natural persons.
Data breach reporting	4. In the case of a personal data breach (see definitions 7): a. Controllers must notify the supervisory authority no later than 72 hours after having become aware of the breach. b. Processors (8) shall notify the controller without undue delay after becoming aware. c. Communicate the data breach to the data subject (exceptions apply).

Category	Requirements
Anonymisation and pseudonymisation	5. Pseudonymisation and anonymisation techniques should be applied: a. As part of the principles of "data protection by design and by default" when processing personal data. b. To data archived with the purpose of public interest, scientific or historical research or statistics.
Cross-border data transfers and binding corporate rules	6. Personal data is subject to transfer restrictions: a. To countries outside the European Economic Area b. Which are not listed as "adequate" Binding Corporate Rules (BCRs) (9) and standard contract clauses (or model clauses) issued by the European Commission remain valid instruments to comply with EU data transfer restrictions (see definitions 10). c. Privacy shield (see definitions 11)
Certifications, codes of conduct and seals	7. Organizations will be able to adhere to certification mechanisms for the purpose of demonstrating the existence of and compliance to certain safeguards.

Definitions taken from GDPR

1. **Data subject.** An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2. **Restriction of processing.** The marking of stored personal data with the aim of limiting their processing in the future.

3. **Controller.** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

4. **Supervisory authority.** An independent public authority which is established by a Member State pursuant to Article 51.

5. **Data Protection Officer.** The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. **Pseudonymisation.** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

7. **Personal data breach.** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

8. **Processor.** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

9. **Binding corporate rules.** Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Additional definitions relevant to GDPR

10. **Adequate countries.** Personal data can flow from the 28 EU countries and three EEA member countries (Norway, Liechtenstein and Iceland) to a third country without any further safeguard being necessary.

    The Commission has so far recognized **Andorra, Argentina, Canada** (commercial organisations), **Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay** as providing adequate protection. (see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

11. To transfer personal data from the EU to the U.S., different tools are available such as contractual clauses, binding corporate rules and the Privacy Shield. If the Privacy Shield is used, U.S. companies must first sign up to this framework with the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles." This department is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles. They must renew their "self-certification" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under the framework. A list of companies that have self-certified to the Privacy Shield can be found on the website of the Department of Commerce (https://www.privacyshield.gov/welcome). A list of companies that are no longer certified under the Privacy Shield is also available.

Section 2:

Requirements

Rights of data subjects

This is one of the most important topics in this regulation. The bar has been raised and new rights have been included that will profoundly impact the way IT will need to process and control personal data. It's important to understand that GDPR is a replacement of the **Data Protection Directive** (Directive 95/46/EC) and its goal is to strengthen and unify data protection for individuals within the EU.

While traditional rights of access (art.15), rectification (art. 16), erasure (art. 17), and objection (art. 21) remain largely the same, a new right has been included: the right to data portability (art. 20) and some modifications to the right to erasure by including the concept of right to be forgotten (art. 17) and the inclusion of right to restriction (art. 18). These rights are fundamental and universal across the EU, where under the previous directive, each member state was allowed to interpret these rights differently, making it hard for the data subjects to claim their rights.

Organizations have multiple challenges and some of the new rights, such as data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services, might be one of the most important. Hence the need to adopt a model that helps companies to cover current and future needs.

When we need to make current applications that include personal data compatible with this new regulation, while at the same time avoiding incurring the cost of modifying existing applications, there's only one answer: APIs.

The adoption of an API-based model for accessing data is the foundation for a future-proof architecture allowing an organization to embrace this regulation and future regulations, not least due to the fact that APIs can be secured, governed and enhanced by implementing appropriate software solutions.

The requirement to obtain consent from the data subject has also been strengthened, so organizations will need to manage their relationship with the data subject in a different manner. Digital identities and their management, governance and access control will play an important role for those who wish to successfully comply with the regulation.

For GDPR compliance, organizations will need to adopt new channels for communicating with data subjects in order to ensure they can properly exercise their fundamental rights. This means that technical measures need to be applied to allow secure and adequate access by the individuals to their data. New channels to allow data portability shall also be created so data subjects might exercise the right of data portability and start the process of transferring their own data to their nominated third party. Thus, it's imperative to deploy appropriate security and sound access controls for these new data gateways.

While it might appear simple, personal data may be accessible across multiple file systems and servers, so proper discovery, analysis and classification has to be applied to the IT infrastructures before even applying data protection policies.

Accountability

Technical requirements are interspersed throughout the regulation, but what it boils down to is "accountability" for the data controller and/or processor. In other words, when incidents occur, as is almost inevitable, the regulator will look for the proof that the company under investigation will have taken the proper organizational and technical controls to ensure proper handling of personal data per the regulation. Organizations need to prove that they have implemented the IT controls and measures required by the regulation, and must continuously monitor and report on all actions taken. Failure to show this will greatly determine the amount of any administrative fine. This is clearly highlighted in article 83.

In the current hybrid IT world, it's not always easy to determine which data in our systems belongs to whom. This might create a challenge to organizations that will need to scan and discover personal data across the full spectrum of existing platforms. In addition, organizations will need to implement solutions to assist not only in identifying the information but helping to control and track the usage of this personal data during the whole lifecycle. Failure to implement technical mature controls in these areas will most likely not lead to any favoritism from the regulator in case of incidents.

Data protection by design and by default

Article 25 recital 2 requires that, "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." And article 30 mandates the recording of processing activities.

Furthermore, article 32, "Security of processing" part (b), requires "… the ability to ensure the ongoing confidentiality, availability and resilience of processing systems and services." Part (d) mandates the existence of "… a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing."

This is a very broad topic that will require a holistic approach ranging from software development processes, including testing, Q&A and the release of new versions. All these IT disciplines will require an embedded layer of security controls to ensure data is accessed only by the right people and for the specific purposes for which it was collected.

Data breach reporting

Derived from the principle of accountability already explained, data controllers and data processors are obliged to report certain data breaches affecting personal data. The types of breaches requiring notice are described in articles 33 and 34.

Article 33 outlines the obligation of reporting data breaches to the competent supervisory authority and article 34 does the same with respect to notice to the data subject. It's important to note that under article 34.3, organizations are exonerated from the obligation to communicate the incident to the data subject if:

- The controller has **implemented appropriate technical and organisational protection measures**, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise.

The communication of a data breach from a processor to a controller must happen without undue delay, and from the controller to the supervisory authority not later than 72 hours after having become aware of it. The report must include information about who did what and when, as well as the actions and measures taken to mitigate any possible adverse effects.

Anonymisation and pseudonymisation

GDPR introduces new concepts related to the principles to be applied when dealing with and processing personal data. Protection of personal data and giving control of it back to the data subject is the main objective of the regulation, so some techniques of protecting personal data are mentioned.

In chapter II ("Principles"), we can see the intention is to strengthen the way personal data is processed ("data minimization") and kept in a form which permits identification of the data subject no longer than is necessary. Also, the personal data needs to be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures ("integrity and confidentiality").

Cross-border data transfers and binding corporate rules

As in the Directive, Article 45 of the regulation puts restrictions on international transfers of personal data to "non-adequate" countries outside the EU. Article 46, recital 2, lays out the appropriate safeguards that need to be in place for data transfer without specific authorization from a supervisory authority.

Binding Corporate Rules (BCRs) (art. 47) and standard contract clauses (or model clauses) issued by the European Commission remain valid instruments to comply with EU data transfer restrictions. Using these transfer mechanisms for intra-group purposes should become easier because certain existing authorization requirements have been dropped. Check definitions 10 and 11 with regards to U.S. Privacy Shield implications.

Controlling who has access to data is fundamental to fulfilling this requirement. Organizations will need to run periodic access-certification campaigns to validate that the access rights for their users are correct at any point in time. The nominated Data Protection Officer (DPO) will need advanced reporting capabilities across different areas of IT security in order to ensure that compliance is met.

In addition, capabilities for restricting the sending of documentation containing personal data outside the organization will need to be used to make sure nobody inadvertently sends files tagged as GDPR-related to third parties that are not authorized.

Certifications, codes of conduct and seals

Organizations are entitled to adhere to certification mechanisms for the purpose of demonstrating the existence of appropriate safeguards. In fact, article 42 has a call to action to the Member States, supervisory authorities and other EU institutions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the regulation. Article 42 also mentions a future framework for a common certification, the “European Data Protection Seal,” which would ensure a common certification standard across the EU, thereby increasing consistency and clarity for citizens.

Section 3:

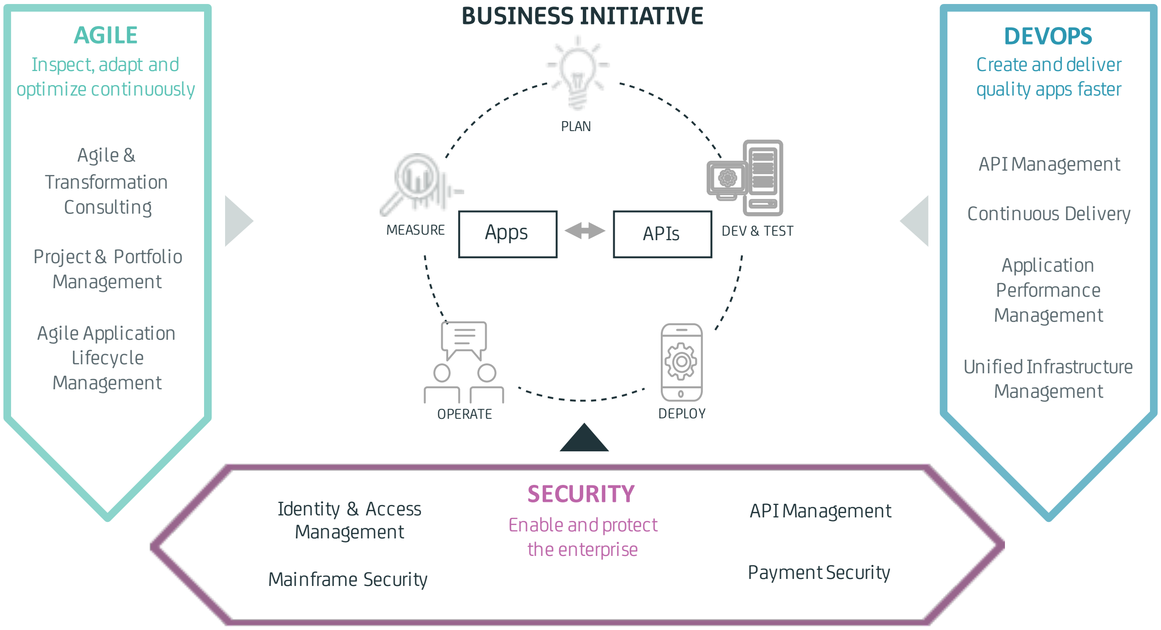
How CA Can Help

Adherence to the regulation will require a thorough approach, including assistance from legal and IT departments, and in some cases consultancy firms, for in-depth assessments and reviews for the regulation itself, as well as for the organizational processes revision. As an innovative software company and leader in the application economy, CA Technologies is guiding organizations through the digital transformation process and can supply a broad set of software solutions to help organizations navigate their compliance journeys.

CA provides the technology organizations need to help achieve GDPR compliance and deploy the necessary controls mandated by the regulation in order to comply with the overall “Security by Default and by Design” philosophy pursued in the regulation.

What separates CA from specific point-technology providers is that our product solutions touch almost every point in an organization’s data lifecycle. The combination of CA solutions for protecting data access, managing and controlling user access, preventing unauthorized access to personal data from outsiders and insiders can be used by organizations in order to ensure adherence to the new regulation by protecting the rights of data subjects. CA Technologies has the tools and expertise to guide organizations through the entire process.

CA Technologies delivers a comprehensive, secure DevOps strategy—one that not only increases the speed of application development and delivery but ensures the security of applications and the entire software delivery lifecycle. Our comprehensive security solutions include API management, mainframe security and several components of our broad IAM security suite. For more information about our IAM security solutions, please visit ca.com/iam.


AGILE
Inspect, adapt and optimize continuously
Agile & Transformation Consulting
Project & Portfolio Management
Agile Application Lifecycle Management
BUSINESS INITIATIVE
PLAN
MEASURE
Apps
APIs
DEV & TEST
OPERATE
DEPLOY
DEVOPS
Create and deliver quality apps faster
API Management
Continuous Delivery
Application Performance Management
Unified Infrastructure Management
SECURITY
Enable and protect the enterprise
Identity & Access Management
Mainframe Security
API Management
Payment Security

CA Technologies on data classification and localisation

While organizations might think they know where personal data is stored and controlled, the reality is that personal data is spread across the organization and widely used, transformed and accessed in different ways by different people, so application-based controls are not enough for complying with the regulation.

Furthermore, the previous Directive was more focused on protecting the files containing personal data and storage of the information, while the new regulation focuses on the processing of the data. This is the result of the new digital age where data is transformed, added, enriched and processed at very high speeds. With modern, big data analytics, seemingly unrelated pieces of data may be combined into personal data that becomes subject to the regulation.

This is why it is extremely important to adopt a defense-in-depth approach for protecting personal data so we can apply different layers of control to it.

Let’s start with the identification and classification of the data as well as understanding the location of personal data in our infrastructure. If personal data is circulating outside the assigned channels and flows, it’s important to understand this and assess the associated risk.

Understanding where personal data lives and who in the organization has access to it is one of the fundamental principles of GDPR.

CA Data Content Discovery

In the application economy, the mainframe is increasingly connected to the rest of the data center, more available to even casual users and subject to data protection regulation. Datasets are copied from production for development or test, then abandoned; others are orphaned as their owners leave the company. In addition, the user-driven injection of unstructured data via UNIX® System Services may have left large volumes of regulated or sensitive data hidden on the mainframe, representing the potential for monetary and reputational damage to the enterprise if it escapes control.

The mainframe still houses over 70 percent of mission-critical data. In fact, if you used your bank debit card, made an airline reservation or a phone call today, chances are you touched a mainframe. But, the application economy has added new risks to the mainframe—it's interconnected to almost all applications, and data breaches are frequently in the news. It would be catastrophic to an organization if the mainframe and its regulated or sensitive data was compromised.

In the current hybrid IT world, it's not always easy to determine which data in our systems belongs to the group affected by the regulation. In order to do this in a proper and systematic manner, **CA Data Content Discovery** finds, classifies and protects sensitive mainframe data in order to cover the full spectrum of existing platforms. The solution includes personal data predefined policies to assist not only in identifying the information but helping to control and track the usage made by the users as mandated in several articles. The scanning is done 100 percent on the mainframe platform, so your data isn't duplicated off-platform for analysis. This allows organizations to quickly identify and protect data before a breach occurs.

CA Identity Suite

Article 25, recital 2 requires that "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." And Article 30 mandates the recording of processing activities. This means that you need to implement a solution that manages and governs proper access of employees to personal data to reduce unnecessary exposure of personal data.

CA Identity Suite helps you manage and govern user access to business applications and the underlying data. The solution supports full compliance with this requirement because it provides reports on who has access to what, and can run and manage access certification campaigns to help enable the organization to stay compliant.

A common approach to compliance is to periodically validate that users have appropriate access to corporate resources. During access certification, managers must review lists of the privileges of their direct reports and either confirm or reject the need for this access.

CA Identity Suite makes this process simple and intuitive, thereby increasing user satisfaction and productivity. Tailoring a certification process to an organization's specific needs is critical to effectively validate access and encourage participation in the process. CA Identity Suite can solicit review from multiple perspectives, such as user managers, resource owners or role engineers. Certification processes, called campaigns, can be executed for each of these perspectives, using different schedules, workflows and approvers. In addition, multiple campaigns can be executed concurrently, each scoped to portions of the organization (e.g., users in a specific business unit) or highlighting different types of access (e.g., only suspected assignments or access gained outside the role model). CA Identity Suite includes robust administrative controls and workflows to help ensure campaigns progress according to requirements. This includes email notifications, reminder alerts and escalation processes for requesting approval from higher-level managers. In addition, when discrepancies are found and changes to access rights are required, remediation processes can be triggered by assigning remediation tickets to the correct owners or through integration with CA Identity Manager.

In this regulation, there is a key actor—the DPO—who must be appointed by organizations. In this role, technological solutions sustaining and demonstrating all the security controls that the organization has put in place to protect personal data will be crucial. The reporting capabilities of CA solutions will help the DPO demonstrate how the organization is adhering to the regulation, and will be relevant for building Data Protection Impact Assessments outlined in art. 35.

CA Identity Suite also includes embedded identity process analytics that provide detailed, easy-to-process information that highlights the operation of key identity processes (such as user onboarding). These analytics help identify and remediate bottlenecks and help ensure that you are meeting your service level agreement commitments. CA Identity Governance includes an extensive set of out-of-the-box reports and dashboards while supporting ad hoc queries for forensic requirements. Reports vary in the level of business and technical information provided in order to address the needs of the different user types. This includes separate reports for business managers, role engineers, compliance officers, auditors and IT personnel, for example.

CA Test Data Management

The regulation is set to have wide-ranging implications for the type of data that can be used in non-production environments. Organizations will need to understand exactly what data they have and who's using it, and must be able to restrict its use to tasks for which consent has been given. One way to avoid exposing personal data to test environments is to not provision it in the first place, even in a masked form. Synthetic data generation offers a technique that could enable organizations to transition to fully virtualized test environments.

When testing and developing software, data can end up spread across test and development as well as complex environments. Testers might copy data to their environment for a given use, but organizations must know how long the data is used for, and that it's used with consent and for a legitimate purpose. Data profiling from **CA Test Data Manager** can help with this key point of compliance by identifying exactly where sensitive data is stored enterprise-wide, and by using statistical analysis to find personal data stored across multiple file formats and applications. Using a cubed view to create an accurate picture of data, CA Test Data Manager identifies sensitive information reflected in related systems, components or applications. Custom, mathematically based filters mean that data can be filtered on a granular level to identify every instance of information relating to an individual. This data can include credit card numbers, email addresses, home addresses and the like, helping organizations fulfil the right to data portability. The data discovery offered by CA Test Data Manager is fully auditable, so that organizations can demonstrate the application of controls taken for compliance.

CA API Management

When we need to make current applications that include personal data compatible with this new regulation, while at the same time avoid incurring the cost of modifying existing applications, there is only one answer: APIs.

The **CA API Management** suite makes it simple for enterprises to address the challenges of information sharing in the application economy. The solution combines advanced functionality for back-end integration, mobile optimization, cloud orchestration and developer management, and is unique in its ability to address the full breadth of these enterprise API management requirements. By using CA API Management, organizations can help demonstrate compliance with the regulation without the need to change current applications. In addition, **CA Live API Creator** can be used to build new APIs that will include the appropriate controls and will expose the information needed to third parties.

For instance, by using CA API Management solutions, we can avoid modifying applications, which is risky and expensive, and will be able to control behaviors from a rule-and-policy-oriented solution. In this way, the organization can incorporate rules for gathering consent, informing users about the information requested by articles 15 and 20 by documenting, through the **CA API Developer Portal**, how the data can be accessed. These security access controls are provided by the **CA API Gateway**.

To understand the benefits of this approach, you can calculate the cost of modifying all applications that currently manage personal data inside your organization, compared to the cost of having one, single, standardized interface that might be also used for complying with other industry regulations.

CA Privileged Access Manager

Whether they're obtained maliciously or used inappropriately by a valid user, exploited privileged user accounts are the common thread of most data breaches. As your environment grows increasingly complex, so does the challenge of defending against ever more sophisticated—and damaging—attacks. Privileged access management from CA offers a comprehensive solution, delivering both network- and host-based controls for the enterprise and hybrid cloud.

While organizations might be tempted to think that protecting access to data through application-based access controls might be enough, the reality is that most data breaches happen by exploiting privileged user accounts, thus surrounding valid access controls and making them useless. This is why organizations need to implement security controls to both manage and govern privileged access.

CA Privileged Access Manager (CA PAM) is a simple-to-deploy, proven solution for privileged access management in physical, virtual and cloud environments. Available as a rack-mounted, hardened hardware appliance, an Open Virtual Appliance (OVA) or an Amazon Machine Instance (AMI), CA PAM enhances security by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity across all IT resources.

A component of CA PAM, **CA Privileged Access Manager Server Control** provides comprehensive protection for your mission-critical servers with powerful, fine-grained controls over operating system-level access and privileged user actions. Capable of enforcing access controls on powerful native superuser accounts—like the UNIX and Linux® root and Microsoft® Windows® administrator—this system-level, host-based solution controls, monitors and audits privileged user activity—improving security and simplifying audit and compliance.

Combining CA Privileged Access Manager Server Control for server hardening with CA Privileged Access Management provides the most complete solution for managing privileged users and access for your organization.

CA Single Sign-On

The application economy has changed the way businesses interact with their customers. Users demand anytime, anywhere access to online services and data, and they expect a seamless and consistent user experience across multiple devices and access channels. With respect to GDPR, organizations need to balance the ease of access against the data that can be accessed. How do you ensure that only the right people are accessing sensitive content, and only when it's legally allowed. For example, an EU citizen has the right to view their personal data; however, can they access and view their data if they are logging in from a country outside the U.S.? What about an employee of the organization? Maybe they can access this same data when logging in from the U.S., but not when they log in from a country outside the U.S.

CA Single Sign-On can manage these challenges by giving employees, customers, partners and suppliers secure single sign-on to online applications, regardless of where they're deployed, what type of device is used to access them or how the user authenticates to the site—directly, via social media or federates in from a partner site. In addition, the solution also enhances security by providing a common policy layer that reduces the possibility of access policy gaps.

GDPR requires that organizations grant access to users but limit the number of people who can access this personal data. A comprehensive access management solution like CA Single Sign-On can provide the appropriate web-access controls for both types of users from a centralized point. Externalizing this security from within the applications supports the security-by-design concept within DevSecOps.

CA Directory

GDPR introduces a major overhaul to existing data protection legislation, and although the majority of this data may exist on mainframes in large enterprises, a significant amount of this data also resides in directories. Organizations are becoming increasingly dependent on their online and mobile applications to provide critical services to their users. And they are facing performance and availability challenges because of issues with the underlying directory infrastructure, including:

- **Explosive Growth.** The explosion of user identities, devices, and the ability to maintain the responsiveness necessary for a superior user experience is challenging many legacy repositories.
- **Identity Silos.** Multiple directories were deployed by different business units over time, which are now causing challenges, including but not limited to, poor user experience, security risk, and increased operational costs.
- **New Requirements.** Security requirements are evolving from simple user authentication to tracking detailed login and personalized information associated with dynamic business operations.

As a result, many customers are looking to elevate their Identity and Access Management infrastructure, migrating to a next-generation directory service that gives better performance at a lower cost of ownership. But GDPR also adds another interesting twist into their evaluation criteria. Your next generation directory service should support the ability to partition the directory tree across multiple servers, which would allow the organization to where personal data is physically stored. In addition, it should also allow you to selective determine which data gets replication across different nodes to prohibit data from leaving a specific region.

CA Cleanup

CA Cleanup identifies accounts unused beyond a specified threshold of time and generates commands to remove unused user IDs, entitlements, permissions and profile and group connections that each user has but doesn't use. The solution helps effectively resolve the accumulation of obsolete and excessive access rights that otherwise occur within a security file over time—a key requirement for compliance with many regulations. CA Cleanup fully deploys within a day and can:

- Identify and remove individual users, entitlements and access groups no longer used.
- Identify entitlements (such as permissions and rules) actually used and create commands to remove those unused. This includes user-defined resources.
- Identify user IDs actually used and create delete commands for those unused. This is based on actual security usage, not reported "last-use" dates, which are often unreliable.
- Produce reports detailing both used and unused entitlements.
- Generate commands to enact or restore security cleanup.

When you use CA Cleanup with CA ACF2™, you can identify active versus inactive logon IDs, rule sets and rules. This includes user-defined resource classes and NEXTKEY source and target rules. When you use CA Cleanup with CA Top Secret®, you can identify active versus inactive ACIDS, permissions and profile connections. This includes user-defined resources and the *ALL* record. When you use CA Cleanup with IBM® RACF®, you can identify active versus inactive user IDs, profiles, permissions, group connections and IBM RACF resource groups. Permission use is tracked down to each specific access-list entry, whether discrete, generic or conditional.

CA Compliance Event Manager

CA Compliance Event Manager provides proactive security monitoring while helping to reduce the cost, complexity and effort required to monitor and report on mainframe security and compliance. With multiple components designed to process information about external security manager events and seamlessly monitor systems for changes to critical resources, CA Compliance Event Manager alerts, inspects and protects mission-essential mainframe data to provide key stakeholders with real-time notifications of potential security breaches.

A large part of GDPR compliance will focus on how data is collected going forward. But a substantial emphasis will fall on the data businesses already hold. With many mainframes containing generations-old data, a manual data audit is completely unrealistic. That's where CA Compliance Event Manager comes in; it offers three critical capabilities:

- **Alert.** The solution monitors entire systems of security records, security configuration points, system data sets and IBM z/OS® configuration controls with real-time and immediate notifications of pertinent violations, access and change activities to critical security systems and resources. This gives stakeholders immediate and critical insights about the potential and magnitude of data exposure on the mainframe to proactively prevent negative security events.
- **Inspect.** Once data exposure threats are identified, CA Compliance Event Manager generates advanced audit and compliance information that isn't available in standard security reports. Through its sophisticated data gathering, comprehensive auditing and data warehouse support, the solution enables users to replay all security events, do forensic analysis with raw security data recording and search, filter and analyse recorded historical data with automatic tape retrieval—all of which provide deeper insights into security and compliance issues and an improved risk posture.
- **Protect.** Once you've received the real-time notifications and inspected the data exposures to quickly triage any issues, you have improved control of your mainframe data and are better prepared to know who has access to GDPR-affected data—from employees to customers and business partners, both past and present—and can make sure appropriate permissions are applied.

Section 4:

Conclusion

GDPR compliance can be achieved through a combination of people, processes and technology. This document has described solutions that can help organizations with their GDPR journey. But you can extend that protection and strengthen security controls even further via strong and risk authentication or workload automation for the processing automation of personal data—helping you comply with GDPR as well as similar mandates. Regulations tend to set the minimum standards to be required, but in the application economy, open enterprises must ensure due diligence to protect one of the most important and critical assets: private customer information.

It's important not to view the GDPR in isolation but in the context of many other laws and regulations—including sector-specific ones—that focus on protecting data in the application economy. Strong controls for the security and protection of data and how it's used and accessed will be critical for organisations seeking to comply with such laws and regulations, regardless of the sector.

View these resources to learn more about CA solutions and the GDPR:

- E-book: “Complying with the EU General Data Protection Regulation. The Implications for Test Data Management”
- White Paper: “EU General Data Protection Regulation (GDPR): Are you ready for it?“

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.