Ten Questions Every Organization Should Ask to Evaluate GDPR Readiness

The deadline for the EU's General Data Protection Regulation (GDPR) is here. Is your organization ready? For many, GDPR will not be a one-and-done, check-the-box project. Rather, it will require continuous investment and adaptation to protect customer privacy and ensure compliance. Here are 10 questions that will help you evaluate where you stand in your GDPR readiness:

1. Can you find your data?

With large amounts of corporate data spread across myriad systems and platforms, manually finding sensitive data is unrealistic. One of your primary technology investments should be toward software that will automatically scan systems to identify the location of sensitive data that has been lost, abandoned or hidden.

2. Can you classify and protect your data?

Once found, the next step is to classify data based on regulation and organizational sensitivity. You can then make business decisions to appropriately secure, encrypt, archive or delete it, and prove to auditors that controls are in place.

3. Can you manage employee access to data?

A common approach to data compliance is to periodically validate that users have appropriate access to corporate resources. During access certification, managers must review lists of the privileged access points of their direct reports and either confirm or reject the need for this access. Additionally, you must be able to demonstrate through reports or access certification campaigns that you are adhering to the regulation.

4. Can you manage your test data?

GDPR impacts the type of data that can used in non-production environments. You need to understand exactly what data you have, who is using it and restrict its use to tasks for which consent has been given. Avoiding using production data in test environments is the best policy. Instead, use synthetic data generation to create is information needed to successfully run tests.

5. Can you manage the applications that process your data?

APIs are the only reasonable way to make current applications that include personal data compatible with this new regulation, while simultaneously avoiding costly modifications to existing applications. APIs can be secured, governed and enhanced by implementing appropriate software solutions.

6. Can you prevent abuses of privileged user accounts?

Reality is that most data breaches are the result of the exploitation of privileged user accounts—whether obtained maliciously or used inappropriately by a valid user. To limit insider threats, you need to implement security controls to both manage and govern privileged access, keeping in mind the principle of least privilege.

7. Can you balance ease of data access with security?

With respect to GDPR, you need to balance ease of access against the data that can be accessed. How do you ensure that only the right people are accessing sensitive data, and only when it is legally allowable? A comprehensive access management solution that includes secure single sign-on capabilities can provide appropriate web-access controls for all users from a centralized point.

8. Can you manage data in directories?

A significant about of personal data resides in directories. Your directory service should allow partitioning of the directory tree across multiple servers, enabling you to specify where personal data is physically stored. It can also help you select how data gets replicated across nodes to prohibit data from leaving a specific region.

9. Can you clean up unused user accounts?

User accounts tend to proliferate, so it is important to identify accounts unused beyond a specified threshold of time and remove unused user IDs, entitlements, permissions and the profile and group connections that each user has but does not use.

10. Can you identify data breaches in real time?

Data breaches will happen—when they do, how soon will you know and take action? Part of your GDPR compliance involves inspecting and protecting mission-essential data to provide key stakeholders with real-time and immediate notifications of pertinent violations, access and change activities to critical security systems and resources.

To learn how CA Technologies can help you comply with many aspects of GDPR, visit **ca.com/gdpr**

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.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy and completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for purpose, or noninfringement. In not event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, good will or lost data, even if CA expressly advised in advance of the possibility of such damages.