DB CyberTech

Technology Brief

Technology Requirements to Remain GDPR Compliant:

- ✓ Continuous Database Asset Discovery
- ✓ Continuous Intelligent Data Classification
- ✓ Continuous Process Mapping of Personal Data on Databases

Foreword

The GDPR (General Data Protection Regulation) was created to harmonize the myriad of data protection laws across the EU. The regulation may impose extremely large fines on companies that improperly manage personal data or fail to continuously protect it. Having a comprehensive and continuous knowledge of where personal data assets are stored is essential to managing this most sensitive data, preventing its loss, responding to change, and avoiding fines.

Databases are information assets that reside at the core of every critical business process. Databases hold high-value company data including personal data. Maintaining an accurate inventory of all assets on databases and the associated personal data they host turns out to be a significant challenge with legacy tools and capabilities. The issue is far larger than a single or even sporadic initiatives to create a personal data inventory. Personal data is dynamic by its very nature. Changes constantly occur in the applications that process personal data, the databases it's stored on, and when it should be destroyed. Therefore personal data needs to be monitored and tracked on a continuous basis. Further, it is necessary to focus beyond just knowing where the databases are; it is also necessary to map and understand who/what is accessing the personal data on those databases, and how the personal data is being processed. Without complete and continuously updated visibility it is not possible to have visibility into personal data assets to protect – resulting in potentially large fines.

GDPR Continuous Compliance

Article	GDPR Requirement	Technology Required
30: Record of Processing Activities	The controller/processor shall maintain a record of processing activities under its responsibility.	Non-intrusive, real-time data mapping and intelligent data classification to enable complete and accurate inventory of processing activities involving personal data.
32: Security of Processing	The controller and the processor shall implement a process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring the security of processing.	Continuous monitoring to enable real-time visibility to the security of the processing of personal data.
33: Breach Notification	The notification shall describe the categories of personal data records concerned.	Predictive behavioral modeling to proactively alert of any potential breach resulting in database data loss, before it happens.
35: Data Protection Impact Assessments	The controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	Intelligent data classification to enable enable assessing the sensitivity and risk associated with any new data processing.
13-15, 17, 20 Rights of the Data Subject	The data subject shall have the right to obtain the categories of personal data concerned.	Non-intrusive, real-time data mapping and intelligent data classification enables effective data minimization.

In order to remain compliant with the GDPR being enacted on May 25, 2018 requires continuous visibility into sensitive assets on the database including the personal data stored there. Structured data in motion requires innovative technology to automate the compliance process. This eliminates much of the manual processes with the associated errors that often results. This will require real-time and non-intrusive monitoring of the conversation between the database and the client. Legacy tools and capabilities do not address these issues effectively in a real-time continuous monitoring environment and have been architected to provide a manual tool to painstakingly identify personal data.

DB CyberTech technology has been architected and developed in conjunction with end user customers including Data Protection Officers and other privacy professionals. The information they need is derived from our deep visibility into database conversations including the ability to accurately and automatically classifying personal data, including previously unknown and undocumented databases. This is accomplished by non-intrusively processing a copy of all database conversations. Deep protocol analysis identifies all assets on all databases, maps databases to their connected applications, and gathers database user behavior analytics. At that point intelligent data classification extracts the meaning of each query and identifies where personal data resides. This inventory is kept up to date in real time, cleanly summarized, easily explored, and quickly exported from the solution.

DB CyberTech enables DPOs and privacy professionals to

- Continuously remain GDPR compliant
- Proactively manage GDPR database requirements for rights of the data subject, records of processing, breach notification, security, and DPIAs to demonstrate compliance when needed
- Respond to end users enquiries
- Demonstrate compliance to auditors
- Reduce risk of fines and legal issues

Conclusion

The GDPR requires companies to have a complete and continuously up to date understanding of their databases and the personal data residing on each of those databases. Legacy tools offer little insight into the applications accessing the databases or the personal data is being used. DB CyberTech has greatly simplified the process of building a comprehensive and continuous inventory of database assets, the clients that connect to them, continuously classifying new data elements, and continuously monitoring personal data on the databases through machine learning. This reduces the efforts associated with managing and protecting personal data. The ability to continuously monitor the conversations between the database and the client for any changes vastly improves the effectiveness of your GDPR compliance initiative.