

DB CyberTech Compliance Solutions: GDPR for Structured Data

Autonomous, Scalable, and Intelligent GDPR Compliance Through Continuous Real-Time Monitoring

GDPR KEY BENEFITS

DB CyberTech enables DPOs and privacy professionals to

- Stay GDPR compliant
- Proactively manage all GDPR requirements for rights of the data subject, records of processing, breach notification, security, and DPIAs to demonstrate on demand compliance as needed
- Respond to end users
- Demonstrate compliance to auditors
- Protect from fines and legal issues

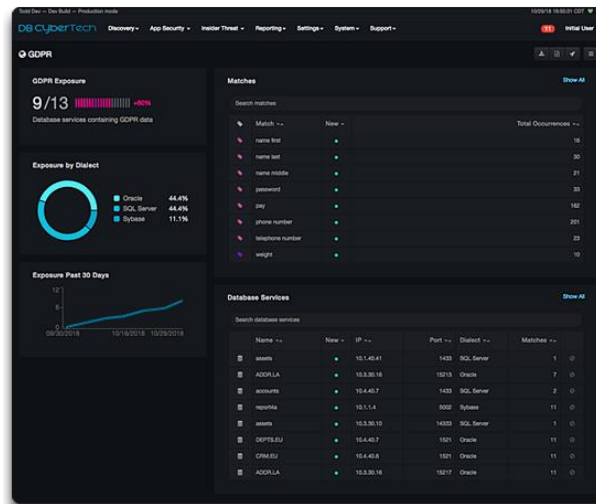
PERSONAL DATA MAPPING

DB CyberTech non-intrusively and automatically discovers

- All structured data assets on the network, including undocumented databases
- All clients accessing databases
- All tables in each database
- All personal data stored or accessed

This information is updated in real time to generate a mapping of personal data in your structured data assets that is

- Complete and accurate
- Provides simple, granular visibility
- Easily searched and exported



- Supports Record of Processing Activities (GDPR article 30) by non-intrusively and continuously classifying personal data in structured data stores and mapping the connectivity of databases with personal data to applications/clients.
- Supports Security of Processing and Breach Notification (GDPR articles 32 and 33) by identifying insider threats and external database attacks with purpose-built predictive detection & alerting of advanced attacks on database and insider threats using machine learning and behavioral analysis.

The GDPR requires that organizations protect personal data – regardless of where the personal data is sent, processed or stored. Companies with employees, customers, or goods for sale in the EU must identify and map the processing all of the personal data they hold and process.

For an effective GDPR program, continuous visibility into an evolving landscape of structured data assets and the personal data stored in them is required. DB CyberTech solves this challenge by automatically decoding and understanding every conversation involving structured data. This capability enables you to efficiently remain GDPR compliant.

DB CyberTech Compliance Solutions supports Data Protection Officers and privacy professionals assembling and maintaining their record of processing activities. We provide visibility to your entire database infrastructure and ferret out personal data in previously unknown databases. This is done by non-intrusively processing a copy of all database conversations. Deep protocol analysis identifies all assets on all databases, maps databases to their applications, and gathers database user behavior analytics (UBA). Then, 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

15015 Avenue of Science :: Suite 150 :: San Diego, CA 92128
www.dbcybertech.com

HIDDEN PERSONAL DATA

DB CyberTech's discovery capability

- Decodes conversations of data in motion
- Goes beyond meta data inspection to understand the semantics of each query
- Decodes obscure and obfuscated references to personal data
- IP address agnostic – it does not rely on IP address or port numbers to identify databases

CONTINUOUS MONITORING

DB CyberTech continuously monitors the network for any changes. This means

- No scanning
- Always up to date
- Complete (never misses a change)
- Immediate notifications via syslog
- Granular visibility for changes in services, clients, applications, and **personal data**

DB CyberTech Enables Key GDPR Requirements

Article	GDPR Requirement	DB CyberTech Response
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 provides 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.	Predictive behavioral modeling gives you alerts of any potential breach resulting in personal data loss from structured data stores, before it happens.
33: Breach Notification	The notification shall describe the categories of personal data records concerned.	Continuous monitoring provides real-time visibility into the database conversations of your processing of personal data. Should a breach occur, any affected personal data can be immediately identified.
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 enables you to assess 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 intelligent data classification and real-time data mapping offers accurate identification of where data subjects personal data is stored reducing the time and cost of supporting data subject requests.

Requirements and Specifications

Supported Database Management Systems

Oracle server release 8i (8.1.7) or later

Microsoft SQL Server version 7 or later

SAP Sybase ASE version 12.5 or later

IBM Db2 Mainframe (DSN)

IBM Db2 LUW (SQL)

DB CyberTech Compliance requires a DB CyberTech Discovery license.

DB CyberTech

15015 Avenue of Science :: Suite 150 :: San Diego, CA 92128
www.dbcybertech.com