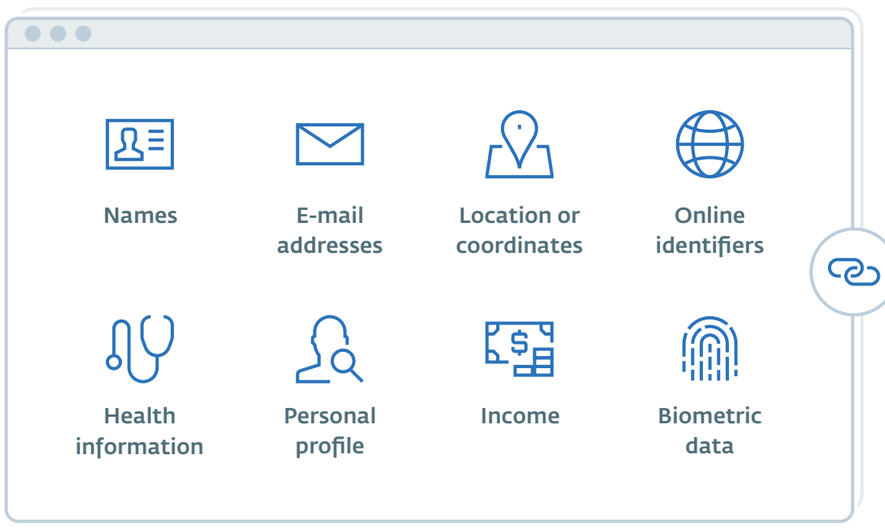
GDPR preparation for your database

STORE THIS IN YOUR DATABASE?

GDPR regulations require that you abide by the rules if you store PII (Personally Identifiable Information).



A JOURNEY, NOT A DESTINATION

GDPR is not a one-time certification.

WHAT IT MEANS FOR YOUR DATABASE?

GDPR brings along some implications and complications for your DB environment.

PREFLIGHT CHECKLIST

Use professional DBA tools to expedite implementation of GDPR governance.

Implement "data protection by design"

Review your database to make sure it's designed in a way that the data is securely and transparently collected and stored with no compromise on functionality.

Map PII to your database objects

Get a detailed report on your database structure and mark all the entities, containing PII. Make sure you have a clear understanding of their critical security parameters and related scripts.

Regularly check database security

Run comprehensive database self-audits regularly to stay aware of potential vulnerabilities. Fix the breaches, if any, before they get exposed.

Monitor vulnerabilities

Detect and clean up inefficient code or orphaned objects to reduce the risk of possible data leaks and improve overall system performance.

Ensure data portability

Individuals could request their data in a commonly used and machine-readable format. Make sure you can generate transparent and comprehensive cross-system exports.

Address PII-related requests

Locate user- and employee-related PII in your database and get ready to address instantly their inquiries and "right to be forgotten" requests.

Facilitate security and data protection

Encryption has been there since early days, but now get ready to pseudonymize a data set. In this case, "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person."

Review your backups

The 'Right to be Forgotten' (RTBF) affects your backups as well. It obliges you to delete every individual-related information you could have. Specifically tricky are legacy applications with archived data, where to delete it, you need to restore it first.

Watch for cross-border data transfers

You must have complete visibility into how scripts, packages or third-party applications could send the data outside of EU area. Generated data exports are becoming extremely vulnerable.

Conquest Software Solutions LLC
6955 N Durango Drive - Ste 1115
Las Vegas, NV 89149
United States

(702) 357-8907

Learn more about GDPR for database professionals at http://sqldev.tech/gdpr