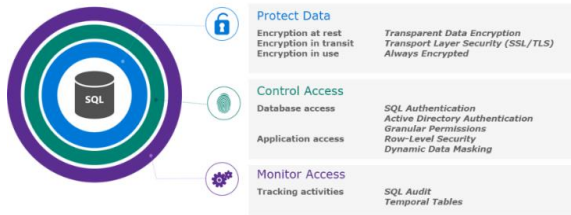


Τεχνολογίες που συμβάλλουν στην συμμόρφωση μιας επιχείρησης με τον GDPR



Extended properties: Δηλώνονται οι στήλες των πινάκων μιας βάσης που περιέχουν ευαίσθητα προσωπικά δεδομένα.

Dynamic Data Masking (DDM): Ενεργοποίηση περιορισμού έκθεσης ευαίσθητων δεδομένων με την αξιοποίηση μασκών σε μη εξουσιοδοτημένους χρήστες από μια βιβλιοθήκη μασκών. Η ενεργοποίηση καλύπτει κάθε δραστηριότητα πρόσβασης (ερώτημα ή προβολή στον πίνακα, stored procedure, εκτύπωση, εργαλεία SQL).



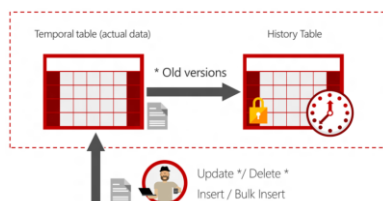
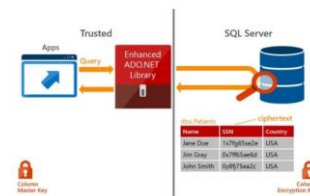
Row-Level Security (RLS): Εναλλακτικός τρόπος περιορισμού της πρόσβασης και ενημέρωσης που αφορά σε συγκεκριμένους χρήστες και σε επιλεγμένα δεδομένα (γραμμές πινάκων).

Transport Layer Security (TLS): Διασφάλιση ότι η μεταφορά των δεδομένων είναι κρυπτογραφημένη (πρωτόκολλο TLS 1.2)

Transparent Data Encryption (TDE): Ένα επιπλέον επίπεδο ασφάλειας είναι η κρυπτογράφηση των δεδομένων "at rest" (TDE). Τα δεδομένα προστατεύονται και σε φυσικό επίπεδο.

Always Encrypted: Το Always Encrypted προσφέρει πλήρη διαχωρισμό των χρηστών σε «ιδιοκτήτες» των προσωπικών δεδομένων και εκείνων που κάνουν επεξεργασία.

SQL Server Audit: Εργαλείο auditing (παρακολούθησης και ελέγχου) σχετικό με τα ευαίσθητα προσωπικά δεδομένα, με πλήρες ιστορικό.



Temporal tables: Υποστήριξη δυνατότητας ιστορικών πληροφοριών επιλεγμένων πινάκων.



Thesis.net GDPR

Η εφαρμογή Thesis.net GDPR αξιοποιεί το σύνολο των παραπάνω τεχνολογιών και εγκαθίσταται σε κάθε προϊόν της οικογένειας Thesis.net (έκδοσης 6.7 η επόμενη) της CGSoft ή των συνεργατών της, όπως ενδεικτικά τα Thesis.net ERP, CRM, Winery, Property & Real Estate Management, Collection, κλπ., δίχως να επηρεάζει την λειτουργικότητά τους. Η εγκατάστασή του Thesis.net GDPR προϋποθέτει συγκεκριμένες προδιαγραφές Server (Microsoft SQL Server 2016/2017) και Client: (.NET 4.6.2, Windows 7 SP1, 8.1 ή 10), καθώς και υπηρεσίες υλοποίησης σε συνεργασία με τον DPO (Data Protection Officer) της επιχείρησης.

Αναλυτικά, οι περιεχόμενες εφαρμογές είναι οι εξής:

Row Level Security (RLS)

Μέσω αυτής της επιλογής συντηρούνται οι πολιτικές (policies) -με εκάστοτε ενεργή μόνο μία, καθώς και οι συνθήκες προσβασιμότητας των χρηστών (Select, Update, Delete, others). Ταυτόχρονα ορίζονται συγκεκριμένοι ρόλοι ή/και οι μεμονωμένοι χρήστες, σε συνδυασμό με τα επίπεδα ασφαλείας (No records, Specific records with criteria, All records). Στη συνέχεια ακολουθεί η ενεργοποίηση του επιλεγμένου policy. Η λειτουργία του **Row Level Security** προσφέρεται σε επίπεδο server και βάσης δεδομένων και είναι ανεξάρτητη (διαφανής) από υπάρχουσες ή μελλοντικές φόρμες (οθόνες) διαχείρισης των προγραμμάτων, εκτυπώσεις, τρίτα προγράμματα ή ακόμη και από το SQL Management Studio.

Dynamic Data Masking (DDM)

Η λειτουργία αυτή ορίζει και παραμετροποιεί τις στήλες εφαρμογής της μάσκας, για τους χρήστες - ρόλους με δικαιώματα πρόσβασης. Η βασική διαφοροποίηση με το Row Level Security είναι πως ενώ το RLS λειτουργεί σε επίπεδο γραμμής πίνακα το DDM εφαρμόζεται σε συγκεκριμένες στήλες της ίδιας γραμμής. Οι μάσκες είναι πολλών ειδών (default(), email, random(), partial() κ.α.). Ένα παράδειγμα μάσκας κάρτας είναι το: '5278 ##### 0000'. Τέλος, οι system administrators έχουν εκ προοιμίου δικαίωμα UNMASK.

Always encrypted columns

Η μέθοδος αυτή επιτρέπει στον client κρυπτογράφηση με απόκρυψη των κλειδιών κρυπτογράφησης από την Database. Η διαδικασία προβλέπει επιλογή των στηλών κρυπτογράφησης που χαρακτηρίζονται από τον τύπο, μήκος, collation, caption, τύπο κρυπτογράφησης (DETERMINISTIC ή RANDOMIZED) τον αλγόριθμο και το κλειδί της κρυπτογράφησης. Επιλέγοντας Always Encrypted και με εγκατεστημένο το πιστοποιητικό (certificate), είναι δυνατή η εμφάνιση των πραγματικών δεδομένων που περιέχονται στις κρυπτογραφημένες στήλες των πινάκων. Για την σωστή λειτουργία του Always Encrypted απαιτούνται ένα πιστοποιητικό (certificate), ένα client master key και ένα column encryption key.

Extended properties - Property names - Property values

Η λειτουργία ορίζει τα αντικείμενα της βάσης δεδομένων που συνδέονται με τα extended properties (π.χ. στήλες πινάκων με ευαίσθητα δεδομένα). Τα αντικείμενα μπορεί να είναι, DATABASE, FUNCTION & FUNCTION PARAMETER, PROCEDURE & PROCEDURE PARAMETER, SCHEMA, TABLE & TABLE COLUMN, TABLE CONSTRAINT, TABLE INDEX, TABLE TRIGGER, VIEW. Σε καθένα από τους τύπους αντικειμένων αντιστοιχίζονται όσα extended properties επιλεγούν. Τέλος εισάγονται οι τιμές των extended properties.

SQL Audit - Server audits & database specifications

Σε αυτή τη λειτουργία εισάγεται ένα audit όνομα και το σημείο αποθήκευσης των δραστηριοτήτων audit (FILE ή APPLICATION LOG). Επίσης συμπληρώνονται τα αντικείμενα (οι πίνακες ή/και οι ρουτίνες) της παρακολούθησης και τα αντίστοιχα events. Αφού ολοκληρωθεί η διαδικασία, ενεργοποιείται από το πεδίο Status. Οποιαδήποτε στιγμή ένα audit μπορεί να είναι είτε ενεργό είτε ανενεργό.

SQL Audit - Read database audits

Η λειτουργία αυτή απεικονίζει όλες τις δραστηριότητες που έχουν καταγραφεί σε όλα τα audits που καταγράφονται σε αρχείο. Για κάθε δραστηριότητα καταγράφεται ο ακριβής χρόνος και ο τύπος της, ο χρήστης, το instance του SQL και η βάση, ο πίνακας, το αντίστοιχο ερώτημα, το όνομα του αρχείου στο οποίο καταγράφηκε και άλλες λεπτομέρειες. Με εφαρμογή κατάλληλων φίλτρων στον παραπάνω πίνακα, ανιχνεύεται ταχύτητα και με ασφάλεια κάθε πρόσβαση, οποιουδήποτε χρήστη, σε οποιονδήποτε πίνακα.



Temporal Tables

Με το SQL audit έχουμε πρόσβαση στις δραστηριότητες των χρηστών πάνω στους πίνακες της εφαρμογής. Για τη δυνατότητα πρόσβασης στις αλλαγές αξιοποιούνται οι temporal tables. Η λειτουργία ενεργοποιείται ή απενεργοποιείται με Status flag, από τον πίνακα παρακολούθησης των ιστορικών δεδομένων.

Temporal Tables - Historical data

Με τη λειτουργία αυτή εμφανίζονται τα ιστορικά στοιχεία κάθε πίνακα που είναι καταχωρημένος στους temporal tables για το διάστημα καταγραφής των στοιχείων. Ανάλογα με τον πίνακα και τον τύπο της εκτύπωσης υποστηρίζονται οι επιλογές: AS OF, FROM, BETWEEN, CONTAINED IN και ALL.

Transport Layer Security (TLS)

Η κρυπτογραφημένη σύνδεση (TLS) εξασφαλίζει πως τα δεδομένα είναι κρυπτογραφημένα κατά τη μεταφορά τους προς και από τη βάση δεδομένων. Για να ενεργοποιηθεί η TLS στον SQL Server, πρέπει να δοθεί πιστοποιητικό στον Server, να διαμορφωθεί κατάλληλα ο Server προκειμένου να δέχεται κρυπτογραφημένες συνδέσεις και τέλος, να γίνει ρύθμιση στις παραμέτρους του client ώστε να απαιτεί κρυπτογραφημένες συνδέσεις. Το ως άνω πιστοποιητικό διατίθεται από αρμόδια αρχή έκδοσης ψηφιακών πιστοποιητικών ή εναλλακτικά από το αυτό-υπογραφόμενο πιστοποιητικό που συνοδεύει τον SQL Server.

Transparent Data Encryption (TDE)

Το TDE υποστηρίζει το σενάριο προστασίας των δεδομένων στο φυσικό επίπεδο αποθήκευσης. Με το συγκεκριμένο χαρακτηριστικό, τα δεδομένα στους πίνακες της βάσης δεδομένων δεν κρυπτογραφούνται άμεσα. Το TDE εκτελεί κρυπτογράφηση και αποκρυπτογράφηση της βάσης δεδομένων, των αντιγράφων ασφαλείας (backup) και των αρχείων καταγραφής των εγγραφών (transaction logs) σε πραγματικό χρόνο, χωρίς καμία ανάγκη αλλαγών στις εφαρμογές. Το TDE προστατεύει τα φυσικά αρχεία δεδομένων (mdf και ldf): αν αυτά μετακινηθούν σε άλλον Server, τότε δεν μπορούν να ανοίξουν και να αξιοποιηθούν. Για την προστασία μίας βάσης δεδομένων με TDE, απαιτούνται τα εξής: α) δημιουργία master key, β) δημιουργία ενός πιστοποιητικού (certificate) το οποίο προστατεύεται από το master key, γ) δημιουργία κλειδιού κρυπτογράφησης της βάσης δεδομένων (database encryption key) το οποίο προστατεύεται από το πιστοποιητικό και δ) ανάλογος ορισμός στη βάση δεδομένων ώστε να χρησιμοποιεί κρυπτογράφηση.