Datenschutz mit SQL Server

– die ganz kurze Version

berndjungbluth.de

Zur Person

- Bernd Jungbluth
  - Freiberuflicher Berater, Entwickler und Trainer
    - SQL Server
    - SQL Server Reporting Services
    - SQL Server Integration Services
    - SQL Server Sicherheitsanalysen
  - Diverse Veröffentlichungen zum Thema SQL Server
    - Bücher, Fachartikel, Vorträge und eigene Seminare
  - Zertifizierter Datenschutzbeauftragter

- Agenda
  - Eine kurze Einführung in die Anforderungen des heutigen Datenschutzes
  - Möglichkeiten von SQL Server zur Umsetzung einiger dieser Anforderungen

Datenschutz

- Was ist Datenschutz?
  - Ein Grundrecht
  - Charta der Grundrechte der Europäischen Union
  - *„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“* (1)
  - Geregelt in der Datenschutzgrundverordnung – EU-DSGVO
  - *„Schützt Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“* (2)
  - Ergänzt durch neues Bundesdatenschutzgesetz – BDSG neu
- Wer muss sich daran halten?
  - Öffentliche Stellen und Unternehmen mit Sitz innerhalb der EU
  - Im europäischen Markt tätige Unternehmen – Marktortprinzip
  - Bei der Verarbeitung personenbezogener Daten

Was sind personenbezogene Daten?

- Informationen zur direkten und indirekten Identifizierbarkeit natürlicher Personen
  - Name, Telefonnummer, E-Mail-Adresse, KFZ-Kennzeichen, Online-Kennung, etc.
  - Interessen, Standortdaten, Bewegungsdaten, Aufzeichnung von Arbeitszeiten, etc.
- Besondere Kategorien personenbezogener Daten
  - Politische Meinungen, biometrische Daten, Gesundheitsdaten, Religion, u. a.
- Besonderer Schutz von Kindern unter 16 Jahren

Was bedeutet *Verarbeiten personenbezogener Daten*?

- Manuelle und automatisierte Vorgänge mit personenbezogenen Daten
- *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang“* (3)
  - Erheben, Erfassen, Speichern, Verändern, Einschränken, Löschen, etc.
  - Auslesen, Abfragen, Abgleichen, Verknüpfen, Offenlegen, Verbreiten, etc.

- Was muss bei der Verarbeitung personenbezogener Daten beachtet werden?
  - Grundsätze zur Verarbeitung personenbezogener Daten
  - Pflichten bei der Verarbeitung personenbezogener Daten
- Welche Grundsätze gibt es?
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - Rechenschaftspflicht

- ## Was bedeutet Rechtmäßigkeit?
  - Grundsätzliches Verbot zur Verarbeitung personenbezogener Daten
  - Erlaubnis nur bei Erfüllen von mindestens einer der folgenden Bedingungen
    - Einwilligung der betroffenen Person
    - Vertragserfüllung und vorvertragliche Maßnahmen
    - Wahrung berechtigter Interessen des Verantwortlichen
    - Rechtliche Verpflichtungen
    - Schutz lebenswichtiger Interessen
    - Wahrnehmung von Aufgaben mit öffentlichem Interesse

- ## Was ist unter Transparenz zu verstehen?
  - Verarbeitung *„in einer für die betroffene Person nachvollziehbaren Weise“* (4)
  - Information der betroffenen Person über die Verarbeitung der Daten

- Was ist eine Zweckbindung?
  - Verarbeitung der Daten nur für vereinbarten Zweck
  - Erhebung der Daten nur *„für festgelegte, eindeutige und legitime Zwecke“* (5)
  - Keine Verarbeitung *„in einer mit diesen Zwecken nicht zu vereinbarenden Weise“* (6)
- Was ist eine Datenminimierung?
  - Verarbeitung der zur Zweckerreichung notwendigen Daten
  - *„dem Zweck angemessen und erheblich“* (7)
- Was ist unter Richtigkeit zu verstehen?
  - Verarbeitung korrekter und aktueller Daten in Bezug auf den Zweck
  - *„sachlich richtig und erforderlichenfalls auf dem neuesten Stand“* (8)
    - Erstellen von Maßnahmen zur unverzüglichen Korrektur oder Löschung unrichtiger Daten

- Was ist eine Speicherbegrenzung?
  - Verarbeitung der Daten nur bis zur Erreichung des vereinbarten Zwecks
  - Erstellen eines Löschkonzepts
  - Unter Berücksichtigung gesetzlicher Aufbewahrungsfristen
- Was bedeutet Integrität und Vertraulichkeit im Datenschutz?
  - Gewährleistung einer angemessenen Sicherheit zur Verarbeitung personenbezogener Daten
  - Erstellen technischer und organisatorischer Maßnahmen
- Was ist eine Rechenschaftspflicht?
  - Einhaltung der Grundsätze
  - Nachweispflicht über die Einhaltung der Grundsätze
  - Erstellen entsprechender Dokumentationen

- Welche wichtigen Pflichten und Aufgaben gibt es?
  - Einhalten der Informationspflicht
  - Erfüllen der Betroffenenrechte
  - Gewährleisten der Sicherheit der Verarbeitung personenbezogener Daten
  - Plus weitere Pflichten und Aufgaben, wie Erstellen einer Vorabkontrolle bzw. einer Datenschutzfolgeabschätzung, Benennen eines Datenschutzbeauftragten, Führen eines Verfahrensverzeichnisses, Sensibilisierung der Mitarbeiter, u.v.m.
- Welche Informationspflichten gibt es?
  - Erfüllen des Grundsatzes der Transparenz
    - Bei Erhebung der Daten
    - Bei Datenschutzverletzungen mit hohen Risiko für die betroffenen Personen
    - Erfüllen der Rechte betroffener Person

Welche Rechte hat eine betroffene Person?

- Auskunftsrecht nach Artikel 15
- Recht auf Berichtigung nach Artikel 16
- Recht auf Löschung nach Artikel 17
- Recht auf Einschränkung der Verarbeitung nach Artikel 18
- Widerspruchsrecht nach Artikel 21
- Recht auf Datenübertragbarkeit nach Artikel 20
- Beschwerderecht bei der Aufsichtsbehörde

Welche Sicherheit der Verarbeitung wird gefordert?

- Erfüllen des Grundsatzes der Integrität und Vertraulichkeit
  - Gewährleisten einer angemessenen Sicherheit zur Verarbeitung personenbezogener Daten
  - Verhindern von Datenschutzpannen durch angemessene Datensicherheit

Was unterscheidet Datensicherheit vom Datenschutz?

- Datenschutz = Schutz natürlicher Personen
  - Betrifft die personenbezogenen Daten eines Unternehmens
- Datensicherheit = Technischer Schutz von Daten
  - Betrifft alle Daten eines Unternehmens
- Enge Verbindung des Datenschutzes mit der Datensicherheit
  - *„Kein effektiver Datenschutz ohne hinreichende Datensicherheit“* (9)
- Datensicherheit durch technisch organisatorische Maßnahmen

Welche Maßnahmen zur Datensicherheit sind gefordert?

- Sicherheit der Verarbeitung personenbezogener Daten – Artikel 32 DSGVO
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung der Systeme – Artikel 25 DSGVO

Was besagt *Datenschutz durch Technikgestaltung*?

- »data protection by design« oder »privacy by design«
- Gewährleisten der Grundsätze des Datenschutzes durch den Einsatz von Technik
- *„zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung“* (10)
  - Bei Planung und Beschaffung sowie beim Design neuer Produkte und Dienstleistungen

Für was steht *Datenschutzfreundliche Voreinstellung*?

- »data protection by default« oder »privacy by default«
- Datenschutzfreundlichste Konfiguration der Systeme als Standardkonfiguration
- Nutzen verfügbarer Sicherheitstechniken als Standardkonfiguration
  - Zweckbindung, Menge der Daten, Zugriffssteuerung, Maskieren von Daten, etc.
- Minimieren der Daten und Maximieren der Sicherheit

Datenschutzpannen, die technisch nicht möglich sind, passieren auch nicht! (11)

Datenschutz mit SQL Server

- Was hat das alles mit SQL Server zu tun?
  - SQL Server = Bestandteil der »Microsoft Data Platform«
  - Produkte und Dienstleistung zur Verarbeitung von Daten
  - Bietet eine Vielzahl von technischen Möglichkeiten zur Datensicherheit
  - Bietet Möglichkeiten zur Umsetzung der Anforderungen vom Datenschutz
- Wie kann SQL Server helfen?
  - Lokalisieren personenbezogener Daten
  - Erfüllen von Betroffenenrechten
  - Einhalten von Grundsätzen zur Verarbeitung personenbezogener Daten
  - Gewährleisten der Sicherheit der Verarbeitung personenbezogener Daten

- Wie lassen sich personenbezogene Daten im SQL Server lokalisieren?
  - Analysieren und Bewerten des Inhalts aller Datenspalten einer Datenbank
    - Analyse der Daten mit SELECT-Anweisungen, Volltextsuche, Fuzzy-Logik, DQS, etc.
    - Analyse anhand der Spaltennamen durch Auswerten von *sys.columns*
    - Mögliche Variante per »Classify Data«
- Empfehlungen
  - Grundsätzliches Kategorisieren und Klassifizieren aller Datenspalten
    - Erstellen eines Metadaten-Katalogs
    - Unterstützung bei der Bewertung durch einen Datenschutzberater
  - Produktivsetzung neuer Datenbanken nur mit entsprechenden Metadaten
    - Nur nach vorheriger Kategorisierung und Klassifizierung der Datenspalten

- Demo
  - Classify Data
  - Auswerten klassifizierter Daten

- Was bietet SQL Server zum Erfüllen von Betroffenenrechten?
  - Auskunftsrecht nach Artikel 15
    - Ausgabe der Information mit SQL Server Reporting Services
  - Recht auf Datenübertragbarkeit nach Artikel 20
    - Sammeln, Aufbereiten und Herausgeben mit SQL Server Integration Services
- Welche Grundsätze zur Verarbeitung unterstützt SQL Server?
  - *Transparenz* durch Ausgabe neu erhobener personenbezogener Daten
    - Voraussetzung: Klassifizierte Datenspalten und Speichern des Anlagedatums
  - *Speicherbegrenzung* durch Ausgabe der zu löschenden personenbezogenen Daten
    - Voraussetzung: Klassifizierte Datenspalten und Speichern des Datums der letzten Änderung
  - *Integrität und Vertraulichkeit* durch Datensicherheit
    - Vielzahl von Funktionen zur Datensicherheit in SQL Server

- Welche Maßnahmen zur Sicherheit der Verarbeitung sind gefordert?
  - Verschlüsseln und Pseudonymisieren
  - Sicherstellen der Vertraulichkeit und Integrität der Systeme und Dienste
  - Sicherstellen der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  - Sicherstellen einer schnellen Wiederherstellung der Systeme und Dienste
  - Prüfen, Bewerten und Evaluieren der Wirksamkeit der Maßnahmen

- Welche Maßnahmen zur Sicherheit der Verarbeitung sind gefordert?
  - Verschlüsseln ~~und Pseudonymisieren~~
  - Sicherstellen der Vertraulichkeit und Integrität der Systeme und Dienste
  - Sicherstellen der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  - Sicherstellen einer schnellen Wiederherstellung der Systeme und Dienste
  - Prüfen, Bewerten und Evaluieren der Wirksamkeit der Maßnahmen
- Was bietet SQL Server im Bereich Verschlüsselung?
  - Symmetrische, Asymmetrische Schlüssel und Zertifikate
  - Ver- und Entschlüsseln von Daten mit T-SQL und »Always Encrypted«
  - Verschlüsseln gesamter Datenbanken mit »Transparent Data Encryption«
  - Verschlüsseln der Kommunikation zwischen Client und SQL Server
  - Verschlüsseln der Datenbanksicherungen

- Was kann SQL Server in Bezug auf Vertraulichkeit und Integrität?
  - Integrität durch Eingabekontrolle und Änderungsnachverfolgung
    - Temporal Tables, Change Data Capture, Change Tracking, OUTPUT und Trigger
  - Vertraulichkeit durch Zugriffsschutz auf mehreren Ebenen
    - Auf Ebene der SQL Server-Instanz und innerhalb der einzelnen Datenbanken
- Zugriffsschutz auf Ebene der SQL Server-Instanz
  - Sicherheit *an* einer SQL Server-Instanz
    - Sicheres Betriebssystem und Dateisystem des Servers für SQL Server
    - Konfiguration der SQL Server-Dienste mit sicheren Dienstkonten
    - Sichere Firewall-Einstellung durch eigens definierte Ports
  - Sicherheit in einer SQL Server-Instanz
    - Anmeldungen und Serverrollen

- Zugriffsschutz auf Ebene der Datenbanken
  - Administrative Rechte an und in Datenbanken
  - Lese- und Schreibrechte in Datenbanken
  - Verschiedene Berechtigungskonzepte realisierbar
    - Zugriff auf Datenbankobjekte per Datenbankrollen
    - Zugriff auf Datenbankobjekte per Schemata
    - Zugriff auf Gespeicherte Prozeduren per Datenbankbenutzer und Schemata
- Zugriffsschutz auf Daten
  - Ausgabe von Datensätzen abhängig von den Rechten des Datenbankbenutzers
    - »Row Level Security«
  - Ausgabe maskierter Daten
    - »Dynamic Data Masking«

- Demo
  - Dynamic Data Masking
  - SQL Server-Konfigurationsmanager und SQL Server-Dienste
  - Standard-Anmeldungen im SQL Server
  - Serverrolle *sysadmin*

- Was bietet SQL Server zur Verfügbarkeit und schnellen Wiederherstellbarkeit?
  - Mehrere bewährte Funktionen zur Ausfallsicherheit
    - AlwaysOn, Datenbankspiegelung, Transaktionsprotokollversand
  - Datenbanksicherung mit eigenen Sicherungsfunktionen
    - Vollsicherung, differenzielle Sicherung und Transaktionsprotokollsicherungen
- Wie lassen sich mit SQL Server die Maßnahmen kontrollieren?
  - Protokollieren nicht erfolgreicher und auch erfolgreicher Anmeldungen
  - Überwachen der SQL Server-Instanz mit »Server Level Auditing«
  - Überwachen von Datenbanken mit »Database Level Auditing«
  - Überwachen eigens ausgewählter Ereignisse mit »Extended Events«
  - Überwachen ausgewählter Konfigurationen mit der Richtlinienverwaltung in SQL Server
  - Anzeigen von Sicherheitsrisiken in Datenbanken mittels »Sicherheitsrisikobewertung«

- Demo
  - Sicherheitsrisikobewertung

- Datenschutz
  - Grundrecht zum Schutz von personenbezogenen Daten natürlicher Personen
  - Schutz natürlicher Personen vor dem willkürlichem Gebrauch dieser Daten durch Dritte
- Datenschutz mit SQL Server
  - Viele Möglichkeiten zur Umsetzung von Anforderungen des Datenschutzes
  - Erfüllen der Rechte *Auskunftspflicht* und *Datenübertragbarkeit*
  - Einhalten der Grundsätze *Transparenz*, *Speicherbegrenzung*, *Integrität und Vertraulichkeit*
  - Gewährleisten der Sicherheit zur Verarbeitung personenbezogener Daten
- Empfehlungen
  - Erstellen eines Metadaten-Katalogs mit klassifizierten Datenspalten
  - Erweitern der Datensätze durch Anlage- und Änderungsdatum zzgl. Benutzerkennung

Danke

Noch Fragen?

✉ *info@berndjungbluth.de*

Vielen Dank für die Aufmerksamkeit.

Quellenangaben

- (1) Artikel 8 Abs. 1 – Charta der Grundrechte der Europäischen Union – (2012/C 326/02)
- (2) Artikel 1 Abs. 2 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (3) Artikel 4 Abs. 2 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (4) Artikel 5 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (5) Artikel 5 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (6) Artikel 5 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (7) Artikel 5 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (8) Artikel 5 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (9) www.wikipedia.de – Artikel *Informationssicherheit* Abschnitt *Datensicherheit*
- (10) Artikel 25 Abs. 1 – EU-Datenschutz-Grundverordnung – EU-Verordnung 2016/679
- (11) Quelle unbekannt