Datenschutz-Grundverordnung und SQL Server

SNEK 6 – April 2018

berndjungbluth.de

Zur Person

- Bernd Jungbluth
- Freiberuflicher Berater und Entwickler
  - Administration SQL Server
  - Entwicklung und Optimierung von SQL Server-Datenbanken
  - Migration Access nach SQL Server
  - Datawarehouse-Systeme
  - SQL Server Reporting Services
  - SQL Server Integration Services
- Kein Datenschutzbeauftragter
- Kein Jurist

Hinweis

Zu Risiken und Nebenwirkungen
lesen Sie die Datenschutzgrundverordnung und
fragen Sie Ihren Anwalt oder Datenschutzbeauftragten.

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

Datenschutz-Grundverordnung

- Datenschutz-Grundverordnung – DSGVO
  - EU-Richtlinie »General Data Protection Regulation« – GDPR
  - *„Schützt Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“* – Artikel 1 (1)
  - Besteht aus 99 Artikel plus 173 Erwägungsgründen
  - Gilt unmittelbar ab 25. Mai 2018
  - Nationale Sonderregelungen durch Öffnungsklauseln möglich
  - Neues Bundesdatenschutzgesetz mit 85 Paragraphen ab 25. Mai 2018
- Geltungsbereich
  - Verarbeitung personenbezogener Daten
  - Öffentliche Stellen und Unternehmen mit Sitz innerhalb der EU
  - Im europäischen Markt tätige Unternehmen – Marktortprinzip

- Personenbezogene Daten
  - Informationen *„auf eine identifizierte oder identifizierbare natürliche Person“* – Artikel 4 (2)
    - Name, Adresse, Telefonnummer, E-Mail-Adresse, Personalausweisnummer, etc.
    - Interessen, Standortdaten, Bewegungsdaten, Online-Einkäufe, Nutzungsprofile, etc.
  - Besondere Kategorien personenbezogener Daten – Artikel 9
    - Politische Meinungen, biometrische Daten, Gesundheitsdaten, Religion, u.w.
  - Besonderer Schutz von Kindern unter 16 Jahren – Artikel 8

- Verarbeiten personenbezogener Daten
  - Manuelle und automatisierte Vorgänge mit personenbezogenen Daten – Artikel 5-11
    - Erheben, Erfassen, Speichern, Organisieren, Ändern, Auslesen, Verwenden, etc.
    - Geregelt durch die Grundsätze zur Verarbeitung personenbezogener Daten

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Grundsätze
  - Grundsätze zur Verarbeitung personenbezogener Daten – Artikel 5
    - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
    - Zweckbindung
    - Datenminimierung
    - Richtigkeit
    - Speicherbegrenzung
    - Integrität und Vertraulichkeit
- Rechenschaftspflicht
  - Einhaltung der Grundsätze
  - Nachweispflicht über die Einhaltung der Grundsätze
    - Erfordert ein Mindestmaß an Dokumentation

- Rechtmäßigkeit
  - Nur bei Erfüllung mindestens einer der im Artikel 6 definierten Bedingungen
    - Einwilligung der betroffenen Person
    - Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen mit der betroffenen Person
    - Wahrung berechtigter Interessen des Verantwortlichen
    - Rechtliche Pflichten, Aufgaben öffentlicher Interessen, Schutz lebenswichtiger Interessen
- Verarbeitung nach Treu und Glauben
  - Unbestimmter Rechtsbegriff
  - *„Verhalten eines redlich und anständig handelnden Menschen“* – Wikipedia (3)
- Transparenz
  - Informations- und Auskunftspflicht gegenüber der betroffenen Person – Artikel 12
    - Offenlegen der zur betroffenen Person gespeicherten Daten

- Zweckbindung
  - Verarbeitung der Daten nur für vereinbarten Zweck – Artikel 5
  - Erhebung der Daten nur *„für festgelegte, eindeutige und legitime Zwecke“* (4)
  - Keine Weiterverarbeitung *„in einer mit diesen Zwecken nicht zu vereinbarenden Weise“* (5)
  - Pflicht zur Benachrichtigung der betroffenen Person bei Zweckänderung
  - Koppelungsverbot – Erwägungsgrund 43
  - Verbot der Abhängigkeit von Erhebung personenbezogener Daten und Vertragserfüllung
- Datenminimierung
  - Nur die zur Zweckerreichung notwendigen Daten – Artikel 5
  - *„dem Zweck angemessen und erheblich“* (6)
  - *„auf die Zwecke der Verarbeitung notwendige Maß beschränkt“* (7)

- Richtigkeit
  - Korrekte Daten in Bezug auf den Zweck der Verarbeitung – Artikel 5
  - *„sachlich richtig und erforderlichenfalls auf dem neuesten Stand“* (8)
  - Erstellen angemessener Maßnahmen
  - Zur unverzüglichen Korrektur oder Löschung unrichtiger Daten

- Speicherbegrenzung
  - Begrenzung der Speicherfrist
  - *„auf das unbedingt erforderliche Mindestmaß“* – Erwägungsgrund 39 (9)
  - Datenhaltung nur zur Erreichung des vereinbarten Zwecks
  - *„wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“* – Artikel 5 (10)
  - Erstellen eines Löschkonzepts
  - Unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen

- Integrität und Vertraulichkeit
  - Gewährleistung einer angemessenen Sicherheit personenbezogener Daten – Artikel 5
  - *„Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“* (11)

- Datenschutz durch Technikgestaltung
  - »privacy by design« – »data protection by design« – Artikel 25
  - Gewährleistung der Grundsätze des Datenschutzes durch Einsatz von Technik
    - Pseudonymisierung, Verschlüsselung, Berechtigungskonzept, Löschkonzept, etc.

- Datenschutzfreundliche Voreinstellungen
  - »privacy by default« – »data protection by default« – Artikel 25
  - Datenminimierung, Speicherfrist, Zugriffsschutz, etc.

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Informationspflichten gegenüber betroffenen Personen
  - Transparente Information und Kommunikation – Artikel 12
  - Informationspflichten bei Erhebung der Daten – Artikel 13 + 14
    - Kontaktdaten des Verantwortlichen, Zweck und Dauer der Verarbeitung, u.a.
  - Mitteilungspflichten zur Ausübung der Rechte der betroffenen Person
    - Recht auf Auskunft, Berichtigung, Löschung, Widerspruch, Beschwerde, u.a.
  - Informationspflichten bei Datenschutzverletzungen – Artikel 34

- Meldepflichten
  - Datenschutzverletzungen bei der Aufsichtsbehörde innerhalb von 72 Stunden – Artikel 33
  - Kontaktdaten des Datenschutzbeauftragten – Artikel 37
    - Angabe bei der Aufsichtsbehörde
    - Allgemein zugängliche Veröffentlichung

- Datenschutzbeauftragter
  - Benennung eines Datenschutzbeauftragen – Artikel 37
  - Behörden und öffentliche Stellen
  - Unternehmen mit bestimmten Kerntätigkeiten
    - Verarbeitung von Daten besonderer Kategorien gemäß Artikel 9
    - Umfangreiche, regelmäßige und systematische Überwachung betroffener Personen
    - Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10

- Bundesdatenschutzgesetz
  - Ergänzung für nicht-öffentliche Stellen
  - *„in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“* – § 38 (12)
  - Plus weitere Kriterien wie Verarbeitung von Daten für Markt- und Meinungsforschung

- Sanktionen
  - Befugnisse der Aufsichtsbehörde – Artikel 58
    - Aussprache von Verwarnungen
    - Anweisung zur ordnungsgemäßen Datenverarbeitung
    - Vorübergehende oder endgültige Beschränkung der Datenverarbeitung
    - Verbot der Datenverarbeitung

- Bußgelder
  - *„in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“* – Artikel 83 (13)
  - Von bis zu 10.000.000 Euro oder von bis zu 2% vom Jahresumsatz letztes Geschäftsjahr
    - Verstöße gegen Artikel 8, 11, 25 – 39, 42 und 43
  - Von bis zu 20.000.000 Euro oder von bis zu 4% vom Jahresumsatz letztes Geschäftsjahr
    - Verstöße gegen Artikel 5 – 7, 9, 12 – 22, 44 – 49, 58 sowie alle Pflichten aus Kapitel IX

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

Personenbezogene Daten

- Personenbezogene Daten
  - Informationen zur direkten und indirekten Identifizierbarkeit natürlicher Personen
  - Betrifft nicht Informationen zu Unternehmen ohne Bezug zu natürlichen Personen
- Herausforderung
  - Lokalisieren personenbezogener Daten
  - Dateien und Systeme wie Dokumente, Bilder, Logdateien, Mailserver, DMS, etc.
  - Daten in Datenbanken wie Spalten mit Namen, Kennnummern, Memofelder, etc.
- Klassifizieren von Daten
  - Analysieren und Bewerten des Inhalts einzelner Datenspalten einer Datenbank
  - Erfüllen von Informations- und Rechenschaftsplichten
  - Realisieren relevanter Maßnahmen wie Löschkonzept, Zugriffsschutz, etc.

- Analyse
  - Bestimmen der Datenspalten mit personenbezogenen Daten – »Data Discovery«
  - Suche anhand der Spalteninhalte
    - SELECT-Anweisungen, Volltextsuche, SSIS mit Fuzzy-Logik, etc.
  - Suche anhand der Spaltennamen
    - Auswerten von *sys.columns* nach Schlüsselbegriffen wie Name, Geburtsdatum, etc.
  - Klassifizieren einzelner Spalten mittels »Classify Data«

- Classify Data
  - Neue Funktion im SQL Server Management Studio seit Version 17.5
  - Ermittelt Spalten mit personenbezogenen Daten anhand der Spaltennamen
  - Erweiterbar mit eigener Auswahl von Datenspalten
    - Zum Kategorisieren und Klassifizieren

- Demo
  - Classify Data

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

Sicherheit der Verarbeitung

- Sicherheit der Verarbeitung
  - Treffen von organisatorischen und technischen Maßnahmen – Artikel 32
  - Gewährleisten eines dem Risiko angemessenen Schutzniveaus
  - Klassifizieren des Schutzbedarfs der personenbezogenen Daten
  - *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos“* – Artikel 32 (14)
- Maßnahmen
  - Pseudonymisieren und Verschlüsseln
  - 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

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Verfügbarkeit und Wiederherstellbarkeit
  - Gesamtheitliches Notfallkonzept
    - Verteilung über mehrere Standorte, Cloud-Lösungen, etc.
  - Möglichkeiten mit SQL Server
    - Hohe Verfügbarkeit mit AlwaysOn
    - Datenbankspiegelung
    - Transaktionsprotokollversand
    - Datenbanksicherung
- Belastbarkeit
  - Im Originaltext »Resilience«
    - Stabilität gegenüber Ausfällen und Angriffen
  - Keine eindeutige Abgrenzung zu *Verfügbarkeit* im Gesetzestext

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Vertraulichkeit und Integrität
  - Grundsatz »Integrität und Vertraulichkeit«
  - *„dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können“* – Erwägungsgrund 39 (15)
  - Zutrittsschutz
  - Zugangsschutz
  - Zugriffsschutz

- Zutrittsschutz
  - Zutritt zum Serverraum
  - Geschützter abgesicherter Raum mit Zutrittskontrolle
    - Biometrischer Zugang, PIN, Kennwort, Schlüssel

- Zugangsschutz
  - Zugang zur IT-Infrastruktur wie Netzwerk und Betriebssystem
  - Authentifizierung per Active Directory und/oder Kerberos
  - Hardwarebasierter Zugangsschutz wie Pin-Eingabe, Biometrie, Kartenleser, etc.
  - Softwarebasierter Zugangsschutz mittels sicherer Kennwörter
  - Aktuelle Updates für Betriebssystem

- SQL Server
  - Aktuelle Cumulative Updates für SQL Server
  - Sicherer Speicherort der Datenbankdateien
  - Sicherer und separater Speicherort der Backup-Dateien
  - Verschlüsselte Datenbanksicherungen

- Demo
  - Backups verschlüsseln

- Netzwerksicherheit
  - Sichere Firewall-Konfiguration
    - Vermeiden von Standard-Ports
  - Deaktivieren nicht verwendeter Netzwerkprotokolle
  - Verschlüsselte Netzwerkübertragung – »Transport Level Security« – TLS
    - SSL-Zertifikat – externes oder selbstsigniertes Zertifikat
- SQL Server-Dienste
  - Beenden bzw. deaktivieren nicht erforderlicher SQL Server-Dienste
    - Aktuell bis zu 11 SQL Server-Dienste zzgl. der CEIP-Dienste
    - Teilweise mit eigenen Berechtigungskonzepten
  - Pro SQL Server-Dienst eigenes Dienstkonto
    - Zuweisen der tatsächlich notwendigen Rechten – »Least Privilege«

- Demo
  - Netzwerkübertragung verschlüsseln

- Zugriffsschutz
  - Zugriff auf Daten
  - SQL Server
    - Mehrstufige Sicherheitsarchitektur
- SQL Server Instanz
  - Authentifizierung per Anmeldekonto – »Anmeldung«
    - Windows-Authentifizierung
    - SQL Server-Authentifizierung
  - Weitere Authentifizierungsmöglichkeiten
    - Asymmetrischer Schlüssel und Zertifikat
  - Steuerung der Rechte durch Serverrollen

- Datenbank und Daten
  - Zugang mittels Benutzerkonto – »Benutzer«
  - Zuordnen eines Anmeldekontos zu einer oder mehrerer Datenbanken
    - Je Datenbank unterschiedliche Rechtevergabe möglich
  - Steuerung der Rechte
    - Benutzer
    - Datenbankrollen

- Datenbankrollen
  - System-Datenbankrollen
    - *public*, *db_owner*, *db_datareader*, *db_datawriter*, *db_denydatareader*, u.a.
  - Benutzerdefinierte Datenbankrollen
  - Anwendungsrollen

- Serverrolle *sysadmin*
  - Administrationsrechte an SQL Server-Instanz
  - Administrationsrechte an allen Datenbanken der SQL Server-Instanz
  - Lese- und Schreibrechte an allen Tabellen der SQL Server-Instanz
- Datenbankrolle *db_owner*
  - Administrationsrechte an allen Objekten und Eigenschaften der Datenbank
  - Lese- und Schreibrechte an allen Tabellen der Datenbank – mit Ausnahme bei DENY
- Empfehlungen
  - Keine Windowsgruppen in Serverrolle *sysadmin*
  - Keine Benutzer mit Anmeldungen auf Windowsgruppen in Datenbankrolle *db_owner*
  - Reduzieren der Anzahl Rollenmitglieder auf das notwendige Minimum

- Demo
  - sysadmin

- Berechtigungskonzept
  - »Separation Of Duties« ~ »Segragation Of Duties«
  - Pro Benutzer eigenes Benutzerkonto
  - Trennen der Aufgaben einzelner Benutzer
- Umsetzung
  - Analyse und Definition von Prozessen bzw. der Aufgaben der Benutzer
  - Trennen der definierten Prozesse von den Benutzern
  - Zusammenfassen der Benutzer in Gruppen
  - Zusammenfassen der Prozesse in Rollen
  - Zuordnen der Gruppen zu den Rollen
  - Erteilen der Rechte für die Rollen an den Objekten der Datenbank
  - Nur die zum Erfüllen der Aufgaben minimal notwendigen Rechte – »Least Privilege«

- Zugriffskontrolle auf Objekte
  - Zugriff auf ein Datenbankobjekt per Datenbankrolle oder Datenbank-Benutzer
  - Umsetzung im SQL Server mittels GRANT, REVOKE und DENY
- Zugriffskontrolle nach Regeln und Eigenschaften
  - Zugriff auf Daten nach definierter Geschäftslogik
    - Regionen eines Bereichsleiters, Ansprechpartner eines Sachbearbeiters, etc.
  - Umsetzung in SQL Server mittels »Row Level Security«
- Zugriffskontrolle durch Datenmaskierung
  - Maskieren von Daten einzelner Spalten
    - Kreditkartennummer, Personalausweisnummer, Gehaltsdaten, etc.
  - Umsetzung in SQL Server mittels »Dynamic Data Masking«

- Row Level Security
  - Zugriffskontrolle auf Datensatzebene
    - Per definierter Geschäftslogik mit Bezug zu den Rechten des Benutzers
  - Umsetzen der Geschäftslogik mittels Tabellenwertfunktion
  - Gewährleisten der Geschäftslogik per Sicherheitsrichtlinie – »Security Policy«
    - »Filter Predicate« zum Filtern der Daten bei der Datenausgabe
    - »Block Predicate« zum Verhindern von nicht erlaubter Datenmanipulationen

- Dynamic Data Masking
  - Maskieren von Daten
  - Definition der Maskierung auf Spaltenebene
    - Gilt grundsätzlich zur Ausgabe der Daten
    - Aufheben der Maskierung durch Vergabe des Rechts UNMASK

- Demo
  - Row Level Security
  - Dynamic Data Masking

Agenda

- Datenschutzgrundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Verschlüsselung
  - Zugriffsschutz durch Verschlüsselung
  - *„Verschlüsselung personenbezogener Daten“* – Artikel 32 (16)
- SQL Server
  - Verschlüsselungsmethoden
    - Symmetrische Schlüssel
    - Asymmetrische Schlüssel
    - Zertifikate
  - Möglichkeiten zur Verschlüsselung
    - Netzwerkübertragung und Datenbanksicherungen
    - Datenbanken mit »Transparent Data Encryption« – TDE
    - Daten mit T-SQL und Always Encrypted

- Verschlüsselungshierarchie im SQL Server
  - Diensthauptschlüssel – »Service Master Key« – SMK
  - Verschlüsselt Informationen der SQL Server-Instanz wie Datenbankhauptschlüssel
  - Datenbankhauptschlüssel – »Database Master Key« – DMK
  - Verschlüsselt Informationen der Datenbank wie Schlüssel, Zertifikate und Daten
  - Sicherungskopien der Schlüssel auf externen Medien sinnvoll

- T-SQL-Funktionen
  - Mehrere Befehle zum Ver- und Entschlüsseln
  - Per symmetrischem Schlüssel mit ENCRYPTBYKEY und DECRYPTBYKEY
  - Per asymmetrischem Schlüssel mit ENCRYPTBYASYMKEY und DECRYPTBYASYMKEY
  - Per Zertifikat mit ENCRYPTBYCERT und DECRYPTBYCERT
  - Per Zeichenfolge mit ENCRYPBYPASSPHRASE und DECRYPBYPASSPHRASE

- Demo
  - Verschlüsseln und Entschlüsseln per T-SQL

- Always Encrypted
  - Ver- und Entschlüsseln der Daten einzelner Spalten einer Tabelle auf Seitenebene
    - Nur möglich mit Zertifikat aus externem Zertifikatsspeicher
  - Erlaubt das Trennen der Datenbesitzer von den Datenverwaltern
    - Nur lesbar für die Applikationen zur Datenverarbeitung
    - Nicht lesbar für Administratoren

- Verschlüsselungshierarchie
  - Spaltenhauptschlüssel – »Column Master Key« – CMK
    - Verschlüsselt Spaltenverschlüsselungsschlüssel
  - Spaltenverschlüsselungsschlüssel – »Column Encryption Key« – CEK
    - Verschlüsselt den Inhalt einer oder mehrerer Spalten einer Tabelle
    - Abhängig von der Verschlüsselungsart *Zufällig* oder *Deterministisch*

- Demo
  - Always Encrypted

- Pseudonymisierung
  - Ersetzen eines Identifikationsmerkmals durch ein Pseudonym
  - Bezüge der abhängigen Daten zum Pseudonym weiterhin vorhanden
  - Begriffsdefinition in Artikel 4
  - „die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“ (17)
  - „sofern diese zusätzlichen Informationen gesondert aufbewahrt werden“ (18)
  - „Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (19)
- Anonymisierung
  - Keine Bezüge der Daten zur betroffenen Person mehr vorhanden
  - Unterliegt nicht der Datenschutz-Grundverordnung – Erwägungsgrund 26
  - *„Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten“* (20)

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Kontrolle der Maßnahmen
  - Gewährleisten der Sicherheit der Verarbeitung – Artikel 32
  - *„Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit“* (21)

- SQL Server
  - Serversicherheit der SQL Server-Instanz
  - Sicherheitsrisikobewertung
  - Überwachungsspezifikationen
  - Richtlinienverwaltung
  - Erweiterte Ereignisse – »XEvents«
    - Zur Konfiguration eigener Überwachungen
  - Änderungsnachverfolgung zur Analyse von historischen Daten
    - »Change Data Capture«, »Change Tracking«, »Temporal Tables«

- Serversicherheit der SQL Server-Instanz
  - Aufzeichnen von Anmeldungen
  - C2-Überwachungsmodus
  - Common Criteria
- Sicherheitsrisikobewertung
  - »Vulnerability Report«
  - Prüft Sicherheitseinstellungen einer Datenbank
  - Liefert ausführlichen Ergebnisbericht
    - Einstufung der ermittelten Sicherheitsrisiken in High, Medium und Low
    - Ausführliche Beschreibung inklusive Empfehlungen zur Korrektur
  - Neue Funktion im SQL Server Management Studio seit Version 17.4

- Demo
  - Sicherheitsrisikobewertung
  - Protokollieren fehlerhafter Anmeldungen

- Überwachungsspezifikation
  - »SQL Server Audit«
  - Serverüberwachungsspezifikationen – »Server Level Auditing«
  - Datenbanküberwachungsspezifikationen – »Database Level Auditing«
    - Seit SQL Server 2016 SP1 in Standard Edition verfügbar
  - Protokolliert Ereignisse in Dateien oder Windows-Ereignisprotokoll
- Richtlinienverwaltung
  - »Policy-Based Management« – PBM
  - Überwachen abweichender Istwerte von definierten Sollwerten
    - Bedarfsgesteuert, nach Zeitplan oder bei Änderung vom überwachten Istwert
  - Automatisierte Kontrolle von Vorgaben bzw. Richtlinien
  - Hinweis im SQL Server Management Studio bei nicht erfüllten Richtlinien

- Demo
  - SQL Server Audit
  - Richtlinienverwaltung

Agenda

- Datenschutz-Grundverordnung
  - Inhalt und Geltungsbereich
  - Grundsätze und Pflichten
- Personenbezogene Daten
- Sicherheit der Verarbeitung
  - Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit und Integrität
  - Verschlüsselung und Pseudonymisierung
  - Prüfung, Bewertung und Evaluierung
- Maßnahmen und Fazit

- Maßnahmen
  - Analyse der Verarbeitung personenbezogener Daten
  - Festlegen eines dem Risiko angemessenen Schutzniveaus
  - Erstellen eines Maßnahmenkatalogs
  - Etablieren der Maßnahmen
  - Regelmäßiges Prüfen der Maßnahmen
- Konkrete Anforderungen
  - Informationspflicht
  - Rechtmäßigkeit der Verarbeitung
  - Rechenschaftspflicht
  - Sicherheit der Verarbeitung

- Datenschutz-Grundverordnung
  - Europaweiter Mindestschutz personenbezogener Daten
  - In Zukunft höhere Priorität für Datenschutz
  - Verleiht dem Datenschutz den ihm gebührenden Stellenwert
  - Klärt Datenhoheit personenbezogener Daten
  - Schützt natürliche Personen vor willkürlichem Gebrauch personenbezogener Daten
- SQL Server
  - Klassifizieren von Daten
  - Verfügbarkeit und Wiederherstellbarkeit
  - Vertraulichkeit, Integrität und Verschlüsselung
  - Prüfung, Bewertung und Evaluierung

Hinweise

- Seminar »Datenschutz mit SQL Server«
  - 2-tägiges Seminar
  - 20. und 21. Juni 2018
  - 799 Euro zzgl. MwSt.
  - Hotel Ebertor in Boppard am Rhein
  - Maximal 8 Personen
  - Exklusive Information für SNEK-Teilnehmer bis 25.04.2018
  - Anmeldung per E-Mail an *workshop@berndjungbluth.de*
- Links
  - EU-DSGVO inklusive Erwägungsgründe und neuem BSDG
  - Microsoft-Website zur DSGVO
  - SQL Server Security

Danke

Noch Fragen?

Vielen Dank für die Aufmerksamkeit.

Quellenangaben

- (1) Artikel 1 Abs. 2 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (2) Artikel 4 Abs. 1 Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (3) „Treu und Glauben“ – https://de.wikipedia.org/wiki/Treu_und_Glauben
- (4) + (5) Artikel 5 Abs. 1 lit. b) Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (6) + (7) Artikel 5 Abs. 1 lit. c) – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (8) Artikel 5 Abs. 1 lit. d) Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (9) Erwägungsgrund 39 – Satz 7 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (10) Artikel 5 Abs. 1 lit. e) Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (11) Artikel 5 Abs. 1 lit. f) Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (12) § 38 Abs. 1 Satz 1 – Bundesdatenschutzgesetz – BDSG
- (13) Artikel 83 Abs. 1 Satz 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (14) Artikel 32 Abs. 1 lit. a) – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (15) Erwägungsgrund 39 – Satz 12 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (16) Artikel 32 Abs. 1 lit. a) – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (17) – (19) Artikel 4 – Abs. 5 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (20) Erwägungsgrund 26 – Satz 7 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung - DSGVO
- (21) Artikel 32 Abs. 1 lit. d)