DSB-5seenland.de

Grundlagen der DSGVO

Ich habe mich mit den Themen Informationssicherheit und Datenschutz schon beschäftigt….

DSB-5seenland.de

intensiv	etwas	gar nicht

Wer hat schon die Meinung gehört, Datenschutz ist nur bürokratischer Unsinn?

Datenschutz? Blödsinn? – Beispiel Verkehr

DSB-5seenland.de

Wie im Straßenverkehr, muss man auch im Datenschutz auf die anderen Teilnehmer achten

Die Regeln sind in der Straßenverkehrsordnung festgelegt. Sie dienen u.a. dem Schutz der körperlichen Unversehrtheit. Sie müssen gelernt und beachtet werden

Auch wenn die Anwendung der Regeln nicht immer einfach ist

Auch im Straßenverkehr gibt es eine „Regelhierarchie", die gelernt werden muss

Wer hat sich schon gefragt, was ein Fachinformatiker mit Datenschutz zu tun hat?

Erwägungsgrund 78 zur DSGVO

… In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, **sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen…**

Umfrage der NOYB-Organisation 2024

Im Frühjahr 2024 startete die österreichische Datenschutzorganisation NOYB des Herrn Schrems eine Umfrage unter 1000 europäischen DSB's wie sie den Stand des Datenschutzes und der DSGVO-Compliance im eigenen Unternehmen einschätzten.
74,4% der Befragten waren der Meinung, dass bei einer Prüfung im Unternehmen gravierende Mängel festgestellt werden würden .
Hauptgründe:

- Mangelnde Aus- und Weiterbildungsmöglichkeiten der DSB
- Zuwenig zeitliche und finanzielle Ressourcen
- Mangelnde Sensibilisierung der Mitarbeiter

Der europäische Datenschutzausschuss EDSA hat daraufhin für 2024 eine generelle Überprüfung des Umsetzungsstandes zur Wahrnehmung der Betroffenenrechte angekündigt.

Die DSGVO im Kontext der Informationssicherheit

DSB-5seenland.de

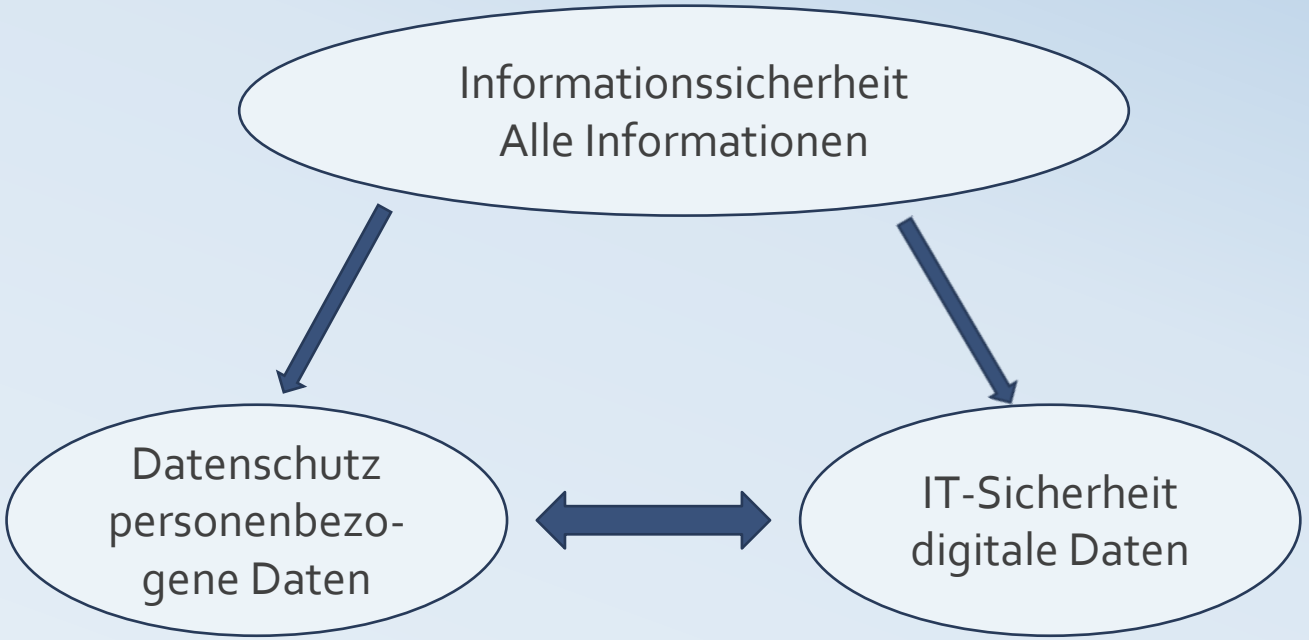
Informationssicherheit
Informationssicherheit hat den Schutz aller Informationen als Ziel, sogen. Schutzziel.
Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein.
Das sind nicht nur Geschäfts-prozesse sondern auch technische/industrielle Prozesse (ICS) und Internet of Things (IoT)

Datenschutz nach DSGVO
Datenschutz hat den Schutz von personenbezogenen Daten als Ziel, sogen. Schutzziel. Auch hier können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein.
Datenschutz ist also Bestandteil der Informationssicherheit

IT-Sicherheit
Diese befasst sich ausschließlich mit der technischen Sicherheit digitaler Informationen. Daher bestehen Wechselwirkungen mit Informationssicherheit und Datenschutz

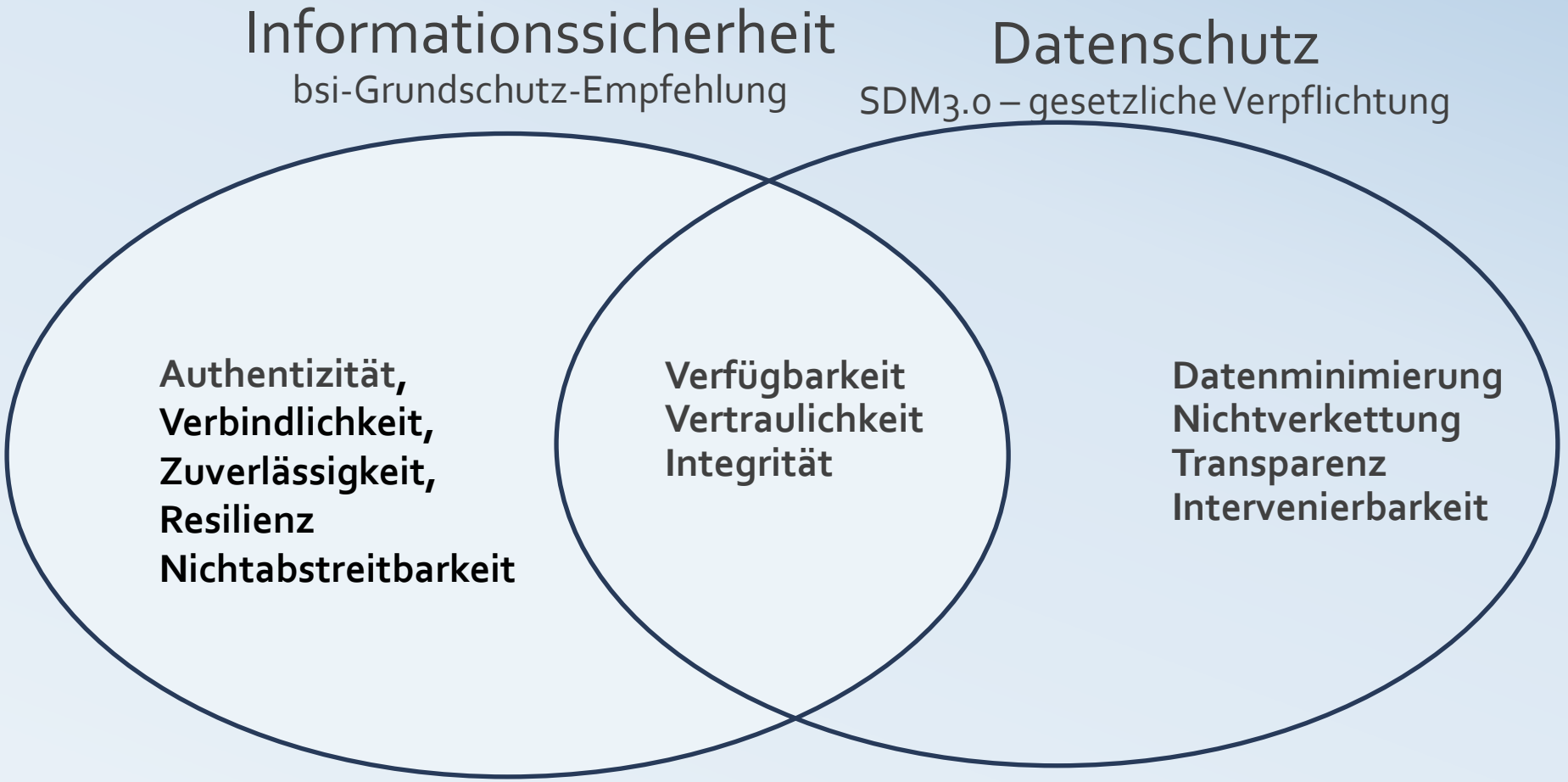
Die DSGVO im Kontext der Informationssicherheit

DSB-5seenland.de



Schutzziele/Gewährleistungsziele

DSB-5seenland.de



Datenschutz – rechtliche Grundlagen

EU-Grundrechte-Charta (GRCh)
Artikel 8 GRCh Schutz personenbezogener Daten

- (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
- 3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Artikel 7 GRCh Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Datenschutz – rechtliche Grundlagen

Grundgesetz der Bundesrepublik Deutschland
Artikel 2, GG

- (1) Jeder hat das Recht auf freie Entfaltung der Persönlichkeit soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt
- (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit Die Freiheit einer Person ist unverletzlich. In diese Gesetze darf nur aufgrund eines Gesetzes eingegriffen werden

Das ist das Recht auf informationelle Selbstbestimmung

Datenschutz – rechtliche Grundlagen

Schutzrechte betreffen i.d.R Eigentumswerte

- Z.B. Recht auf Schutz meines Autos gegen Diebstahl/Beschädigung
- Z.B. Recht auf Schutz meiner Wohnung gegen Einbruch etc.
- Z.B. Schutz der körperlichen Unversehrtheit

- **Für alle diese WERTE gibt es gesetzliche Bedingungen, was erlaubt ist und was bestraft werden kann.**

Im Datenschutzkontext bedeutet das…..

- Personenbezogene Daten sind persönliches Eigentum der betroffenen Person
- Sie haben also einen Wert

- **Auch für diese WERTE gibt es gesetzliche Bedingungen, was erlaubt ist und was bestraft werden kann – DSGVO, BDSG und mitgeltende Gesetze**

Reichweite der DSGVO

Artikel 2 –Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten…

a. ……

b. ……

c. durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Familienprivileg),

d. durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Reichweite der DSGVO

Artikel 3 – Räumlicher Anwendungsbereich

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

   a. betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

   b. das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Datenschutz – rechtliche Grundlagen

Europäisches Recht

DSGVO – Umsetzung
zum 25.5.2018

Deutsches Recht (ergänzend)

Bundesdatenschutzgesetz
(BDSG) von 2018

Bundesdatenschutzgesetz (BDSG) von 2018

Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch
1. **öffentliche Stellen des Bundes,**
2. **öffentliche Stellen der Länder,** soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
a) Bundesrecht ausführen oder
b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

Für nicht-öffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, **es sei denn,** die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich **persönlicher oder familiärer Tätigkeiten**.

Datenschutz – technische Grundlagen

DSB-5seenland.de

Bsi-Grundschutz

- Bsi-Grundschutzkompendium_2023
- Bsi-Standard 200-1 ISMS
- Bsi-Standard 200-2 Grundschutzmethodik
- Bsi-Standard 200-3 Risikoanalyse
- Bsi Standard 200-04 Business Continuity

DSGVO

- Art.32 TOM – technisch-organisatorische Maßnahmen
- Standarddatenschutzmodell SDM3.0

Die 3 großen Irrtümer

DSB-5seenland.de

Wir sind zu klein, die DSGVO trifft auf uns nicht zu

Das trifft auf so gut wie kein Unternehmen oder Selbst-ständigen zu. Sobald personenbezogene Daten von Kunden, Mitarbeitern, Lieferanten oder Bewerbern digital oder analog (im Ordner, im Terminbuch) gespeichert oder verarbeitet werden, muss der Verant-wortliche für einen angemes-senen Schutz dieser Daten sorgen und unterliegt den Vorschriften der DSGVO.

Wir müssen keinen Daten-schutzbeauftragten benennen, also müssen wir auch keinen Datenschutz betreiben

Die Verpflichtung zum Datenschutz ist völlig unabhängig von der Bestellung eines Datenschutz-beauftragten.
Sie richtet sich ausschließlich danach, ob personen-bezogene Daten erhoben, gespeichert oder verarbeitet werden. Unabhängig von der Größenordnung und der Art der Verarbeitung

Die DSGVO ist eine unnötige Kostenbelastung – wer bei uns kauft, braucht keinen Datenschutz

Immer wieder wird kolportiert, dass die DSGVO gerade für kleine Unternehmen ein reines Bürokratiemonster sei. Aber, unbesehen der gesetzlichen Vorschriften:

- Angesichts der ungehemmten Daten-sammelwut vieler Unternehmen ist dies ein Schritt zu mehr Schutz des einzelnen Bürgers vor dem Missbrauch seiner persönlichen Daten.
- Für den normalen Kleinunternehmer ist das ein einmaliger Kraftakt, der mit gesundem Menschenverstand in erträglichem Rahmen gehalten werden kann
- In manchen Fällen kann der Verweis auf volle DSGVO-Konformität auch ein Wettbewerbs-vorteil sein