Datenschutz

In Industrie 4.0

Rechtlichen Rahmenbedingungen

- Geregelt im BDSG-neu durch die Umsetzung der DSVGO, die seit dem 25. Mai 2018 in Kraft ist

Grundsätze

Verbot mit Erlaubnisvorbehalt

- Generelles Verbot der Datenerhebung mit gesetzlichen Ausnahmen
- Daten nach Ablauf der Notwendigkeit direkt löschen
- Ausgenommen sind aufbewahrungspflichtige Daten

Zweckbindung

- Erhebung ausschließlich für die vertraglich festgehaltenen Bedingungen (den Zweck) erlaubt
- unmittelbar danach Löschungspflichtig
- Weitergabe an Dritte verboten
- Ausgenommen für die Strafverfolgung, und Abrechnung

Datenminimierung

Es dürfen auch nur die für den Zweck benötigten Daten verlangt werden.

Transparenz und Hinweispflicht

- leicht verständliche Sprache
- Aufzählung aller Daten nach Art, Umfang und Verwendung
- Datenschutzeinwilligung der Nutzer vor außerrechtlicher Datenerhebung
- Möglichkeit jederzeit zu widersprechen
- Alle Datenschutzmaßnahmen müssen im sog. Verarbeitungsverzeichnis dokumentiert werden

Vertraulichkeit

- Schutz vor Verarbeitung, Veränderung, Vernichtung oder Diebstahl anderer, technisch und organisatorisch
- keine klaren Handlungsempfehlungen der DSVGO
- mehr Schutz ist immer besser
- Im Zweifel entscheidet ein Gericht, ob die ergriffenen Maßnahmen ausreichend waren

Meldepflicht

Datenpannen müssen innerhalb von 72 Stunden nachdem sie dem Unternehmen auffallen an die Betroffenen und die zuständige Behörde gemeldet werden.

Kopplungsverbot

Unternehmen dürfen Leistungen nicht mit der Einwilligung zur Abgabe von Daten, die für die Leistung nicht erforderlich sind, verpflichten.

Auftragsverarbeitung

- externes Unternehmen verarbeitet Daten des Nutzers
- Verantwortung liegt beim Webseitenbetreiber
- Vertrag über die Verarbeitung und Übertragung
- Genaueres in Art. 28 geregelt wie

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten.

Datenarten

An die Sicherung der gespeicherten Daten werden unterschiedliche Anforderungen nach ihrer Art gefordert

personenbezogenen Daten

- Beschreiben eine natürliche Person
- Beispiele: Name, Geburtsdatum, Adresse, Bankdaten, IP-Adressen, Cookies, Geschlecht etc.

Besonders personenbezogene Daten

Ethnische und kulturelle Herkunft, alle politischen, religiösen und philosophischen Ansichten, genetische und biometrische Daten wie Fingerabdruck, Venen oder Iris. Sie sind besonders zu schützen.

Unterscheidung

- Alles gleich gut sichern?
- Datensicherheit kostet Performance

Umsetzung in der Datensicherheit

- wie die Daten geschützt werden
- alle Daten werden geschützt
- Vertraulichkeit
- Integrität
- Verfügbarkeit durch „Data Loss Prevention (DLP)“[1]

Prinzipien

„Privacy by Design“

- Datenschutz von Anfang an mit einbauen
- Mit möglichst wenig Daten auskommen können

[1] Vgl. Probleme mit der Datensicherheit (e-commerce-Magazin.de)

„Privacy by Default“

- Datenschutz freundlichste Einstellung als Standard

Datenschutz-Folgeabschätzung (DSFA)

- Risiko-Abschätzung
- Besonderer Schutz
    - Im Cloud-Computing
    - Bei medizinischen Daten

TOM

- Technische und organisatorische Maßnahmen

Unterschied

Technische Maßnahmen	Organisatorische Maßnahmen

- bauliche Maßnahmen
  ○ Umzäunung des Geländes
  ○ Sicherung von Türen und Fenstern
  ○ Alarmanlagen
- Soft- und hardware-Maßnahmen wie
  ○ Benutzerkonto
  ○ Passworterzwingung
  ○ Logging (Protokolldateien)
  ○ biometrische Benutzeridentifikation
	- Handlungsanweisungen, Verfahrens- und Vorgehensweisen umgesetzt
	  ○ Besucheranmeldung
	  ○ Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
	  ○ Vier-Augen-Prinzip
	  ○ festgelegte Intervalle zur Stichprobenprüfungen

Schutzmaßnahmenkategorien

Zutrittskontrolle	Verhindern, des Betretens des Geländes
Zugangskontrolle	durch Authentifizierung an den Geräten
Zugriffskontrolle	Berechtigungen der Mitarbeiter und Schutz vor Kopie der Daten
Weitergabekontrolle	Bei der Weitergabe der Daten darf nicht mitgelesen werden
Eingabekontrolle	Nachvollziehung der Eingabe, Änderung der Daten: Protokolle, Versionsverlauf
Auftragskontrolle	Prüfung, ob sich an die Verträge gehalten wird: z. B. Stichproben
Verfügsbarkeitskontrolle	Backups, Schutz vor Zerfall, Zerstörung
Trennungsgebot	Trennung nach unterschiedlichen Zwecken

Verschlüsselung

- Informationen für unbefugte unlesbar machen
- Dafür wird ein Schlüssel (automatisch) festgelegt
- Mit Verschlüsselungsalgorithmen (Bsp. SSL, RSA, AES, Blowfish, Twofish)

Kerckhoffsches Prinzip

- „Die Sicherheit eines Kryptosystems hängt einzig und allein von der Geheimhaltung des Schlüssels ab.“
- Die Verschlüsselungsalgorithmen sind bekannt
- Berechenbar durch die Kombinatorik (12.2 Stochastik)

Faktor Mensch

- Größtes Sicherheitsrisiko
- Schulung

Veränderungen für Stakeholder

Alle

- Profitieren von ihrer Datensicherheit im Kontakt mit dem Unternehmen
- Daten sind ein wichtiges zu schützendes Gut (festgehalten im Grundgesetz)

Aktionäre

- Erhalten mehr Rendite, da das Unternehmen keine teuren Gerichtsprozesse und Strafen zahlen muss, wenn gesetzliche Vorgaben eingehalten werden

Mitarbeiter

- Großer Aufwand die Maßnahmen umzusetzen, der auch keinen Spaß macht
- Erhalt des Arbeitsplatzes, da das Unternehmen keine Strafen zahlen muss

Lieferanten

- Halten sich dadurch an ihre Datenschutzregeln (s. o. Auftragskontrolle)
- Mehr Einnahmen durch Datenschutz notwendige Güter

Kommune

- Glücklichere Einwohner, deren Daten geschützt sind
- Steuereinnahmen, da das Unternehmen nicht Pleite geht
- Weniger Arbeitslose

Manager

- Aufwand wegen der Koordination
- Muss sich fortbilden (lassen)
- Muss den Aktionären die Kosten schön reden

Staat

- Hat weniger Aufwand im Bereich der Strafverfolgung
- Wird von anderen Staaten ernst genommen, da seine Gesetze auch umgesetzt werden

Kunden

- Müssen die Kosten tragen (Internalisierung der Kosten)

Gläubiger

- Unternehmen bleibt erhalten, sodass die Verbindlichkeiten irgendwann zurückgezahlt werden

Wir danken Euch für Eure Aufmerksamkeit.

Fragen beantwortet Jakob gerne.

Für mehr Informationen besuche JbSchmitt.de