datenschutz by migosens

DATENSCHUTZ IM SMART BUILDING – WAS MUSS BEACHTET WERDEN

Webinar
27. November 2020

Heiko Gossen, migosens

Die schlechte Nachricht zuerst!

„Bei den Verbrauchsdaten handelt es sich um personenbezogene Daten, da diese Rückschlüsse auf das Heizverhalten der Wohnungseigentümer, die Zeiträume ihrer An- und Abwesenheit und die Nutzung bestimmter Räume ermöglichen.“

LG Dortmund, Urteil vom 28.10.2014 - 9 S 1/14

Aber:
Deswegen müssen wir nicht aufgeben!

Vorstellung Speaker

HEIKO GOSSEN
Geschäftsführer

migosens GmbH
Wiesenstraße 35
45473 Mülheim an der Ruhr
Tel. 0208 / 99395110
heiko.gossen@migosens.de

Datenschutzauditor (TÜVCert)

Lead Auditor ISO 27001 i.A. der TÜV Rheinland Cert GmbH

ehem. Datenschutzbeauftragter der Telefónica Deutschland GmbH und Postbank Systems AG

Network Security Engineer

Mitglied des Vorstands im Arbeitskreis Datenschutz des Bitkom e.V.

https://www.linkedin.com/in/heiko-gossen-2a5a9a1b7/

https://www.xing.com/profile/Heiko_Gossen

Ihr Spezialist für Datenschutzmanagement, Informationssicherheit und IT & Business

datenschutz by migosens

„UNSERE MITARBEITER SIND **JURISTEN**, **TECHNIKER**, **INFORMATIKER**, **KAUFLEUTE UND PROZESSMANAGER**. SOMIT KÖNNEN WIR ALLE ASPEKTE EINER FACHLICHEN HERAUSFORDERUNG UMFASSEND BETRACHTEN UND LÖSUNGEN MIT WEITBLICK ANBIETEN."

Heiko Gossen, Geschäftsführer

Unser Serviceportfolio gliedert sich in vier Bereiche

datenschutz by migosens

migosens

datenschutz

Beratung

Audits (intern/extern)

Externer DSB

TK-Datenschutz

managementsysteme

Beratung
(27001 / 9001 / 22301)

Audits (intern)

Externer ISB / QMB

Einführung ISMS
QMS und i DSMS²

akademie

DSB-Ausbildung

Projekte und Prozesse

Informationssicherheit

Integrierte Managementsysteme

worksmart

Führung und Zusammenarbeit

Organisationsentwicklung

Arbeitsumfeld gestalten

ERFAHRUNG. WISSEN. BERATUNG.

Anforderungen an eine datenschutzkonforme Verarbeitung

datenschutz by migosens

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Vertraulichkeit und Integrität

Welche Fragen muss ich beantworten?

datenschutz by migosens

Wichtige Fragen auf dem Weg zur rechtmäßigen Datenverarbeitung

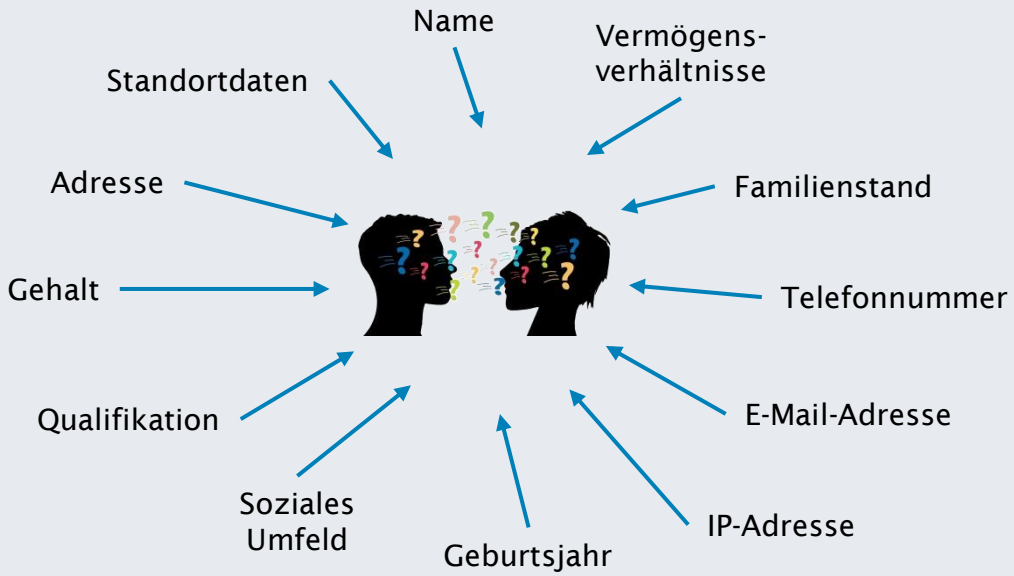
1. Benötige ich eine Rechtsgrundlage und habe ich eine?
2. Sind alle Daten zur Erreichung des Zwecks erforderlich?
3. Wie lange darf ich die Daten aufbewahren?
4. Wie sind Dienstleister vertraglich verpflichtet?

Datenschutzrelevanz

datenschutz by migosens

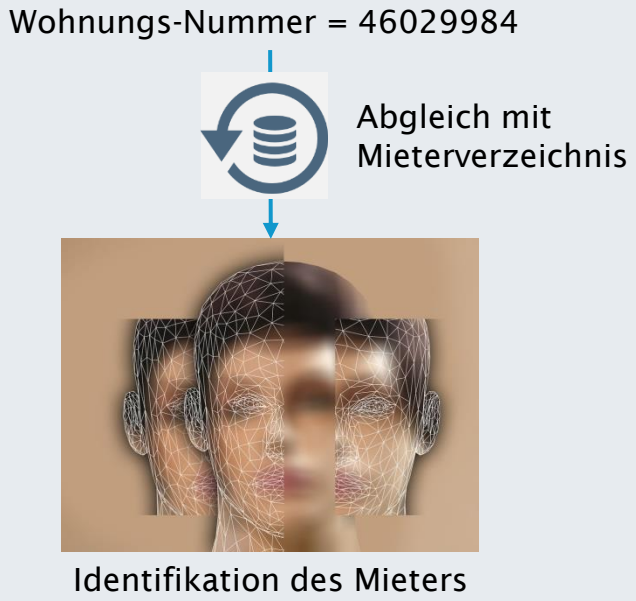
Personenbezogene Daten (Art. 4 Abs. 1 DSGVO)

- Alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** („betroffene Person“) beziehen



Identifizierbarkeit

- **Identität** einer Person **durch Kombination** der Daten mit einer anderen Information **feststellbar**



Benötige ich eine Rechtsgrundlage und habe ich eine?

datenschutz by migosens

Grundsatz (Art. 5 DSGVO)
• Personenbezogene Daten müssen rechtmäßig und auf eine für den Betroffenen nachvollziehbare Weise verarbeitet werden • Die Erhebung darf nur zu vorab festgelegten, eindeutigen und legitimen Zwecken erfolgen

Mögliche Rechtsgrundlage	Beispiel
Einwilligung	Telefonische Werbeansprache
Für die Erfüllung **eines Vertrages** erforderlich	Beschäftigungsverhältnis, Kaufvertrag oder Mietvertrag
Zur Erfüllung **rechtlicher Pflichten** des Verantwortlichen erforderlich	Meldung an Sozialversicherungsträger, Finanzamt
Zur Wahrung **berechtigter Interessen** erforderlich *soweit* keine Interessen/Grundrechte/Grundfreiheiten des Betroffenen überwiegen	Briefwerbung an Bestandskunden, sofern diese nicht widersprochen haben

Anforderungen an eine wirksame Einwilligung

datenschutz by migosens

- **Anforderungen** an die wirksame Einwilligung:
  - ✓ **Freiwillig** und **für einen bestimmten Fall**
  - ✓ Hinreichende **Information** betroffener Person + Einwilligung muss **unmissverständlich** abgegebene Willensbekundung sein
  - ✓ Widerruf jederzeit möglich und Betroffener muss vorab darauf hingewiesen werden
- Immer Prüfung, ob es eine Alternative zur Einwilligung gibt
  - ✓ Rückgriff auf andere Rechtsgrundlagen im Falle einer verweigerten Einwilligung ist in der Regel nicht möglich

Beispiel 1

Bei Webformularen darf die Checkbox für die Einwilligung nicht vorausgewählt sein.

Beispiel 2

Die Einwilligung im (neuen) Mietverhältnis sollte kritisch hinsichtlich der Freiwilligkeit geprüft werden.

Sind alle Daten zur Erreichung des Zwecks erforderlich?

datenschutz by migosens

Datensparsamkeit / Datenminimierung

- Personenbezogene Daten müssen für den Zweck angemessen und erforderlich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- Beispiel (erlaubt):
  Die Erfassung der Anschrift-Daten für die Lieferung von Waren
- Beispiel (nicht erlaubt)
  Die Erfassung von Hobbies beim Online-Kauf als verpflichtende „Zusatzangabe“

Datenminimierung durch Aggregation

- Sofern personenbezogene rechtmäßig erhoben werden, kann Datenminimierung auch durch Aggregation erfolgen.
- Beispiel: Unverzügliche Löschung der Rohdaten nach Aggregation

Wie lange darf ich die Daten aufbewahren?

datenschutz by migosens

Löschung von Daten

- Personenbezogene Daten müssen in der Regel gelöscht werden, wenn
  - der Zweck, für den sie verarbeitet wurden, erfüllt ist und keine gesetzliche Pflicht zur Aufbewahrung besteht
  - die zugrunde liegende Einwilligung widerrufen wird
  - die Daten unrechtmäßig verarbeitet werden.
- Eine hinreichende Anonymisierung kann eine Löschung ersetzen.
- Eine Pseudonymisierung oder Sperrung kann eine Löschung **nicht** ersetzen.

Was bedeutet Löschen?

datenschutz by migosens

Eine Wiederherstellung darf nicht möglich sein!

Auch Backups und archivierte Dateien müssen regelmäßig gelöscht werden!

Die Löschung sollte nach festgelegten Fristen automatisch erfolgen!

Anonymisierung kann Löschung ersetzen…
- Am besten über Aggregation der Daten
- Hinreichende Anonymisierung von Einzeldatensätzen ist sehr aufwendig, da alle vorhandenen Informationen betrachtet werden müssen

Löschen von Daten

Hinweise

- Löschfristen sollten auch Aufbewahrungspflichten berücksichtigen!
- Festlegung der Fristen sollten in Abstimmung mit dem Datenschutzbeauftragten erfolgen!

Wie sind Dienstleister vertraglich verpflichtet?

datenschutz by migosens

Dienstleisterauswahl

- Das beauftragende Unternehmen (der Verantwortliche) bleibt verantwortlich für den Datenschutz – auch bei Einbindung von Dienstleistern.
- Dienstleister müssen daher immer sorgfältig ausgesucht und ggf. vorab überprüft werden.
- Die Beauftragung von Dienstleistern außerhalb der EU/EWR ist erfahrungsgemäß aufwendiger.
- Auch innerhalb eines Konzerns sind entsprechende Regelungen zu treffen.

Grundsätze der Auftragsverarbeitung & Pflichten des Verantwortlichen

datenschutz by migosens

GRUNDSÄTZE

- **Verpflichtung des Auftragsverarbeiters** bzgl. Gegenstand und Dauer der Verarbeitung
- **Konkretisierung der Art** der personenbezogenen Daten sowie der Kategorien der Betroffenen
- **Vereinbarung von Pflichten & Rechten** des Verantwortlichen und des Auftragsverarbeiters
- **Vertrag in Textform** (Schriftform, elektronische Form)

Auftragsverarbeitungs-vereinbarung →  → Vertrag zwischen den Parteien

- **Dokumentierung erteilter Weisungen** für die Datenverarbeitung des Verantwortlichen sind **Voraussetzung für eine rechtskonforme Auftragsverarbeitung**
- **Weisungen** müssen sich **im Rahmen des gesetzlich Erlaubten** bewegen

→ Erteilung dokumentierter Weisungen

PFLICHTEN

Sorgfältige Auswahl des Dienstleisters ←

- **Fachwissen, Zuverlässigkeit und Ressourcen** des Auftragsverarbeiters sind **Indizien**
- **Verstoß** gegen eine sorgfältige Auswahl ist **bußgeldbewehrt**

Garantien des Dienstleisters ←

- Überprüfung der technischen und organisatorischen Maßnahmen des Dienstleisters, z.B. anhand von Zertifikaten oder internen Testaten

Usecase 1: Heizkostenerfassung

Erfassung Verbrauchsdaten
Heizkörper
im 15-Minuten-Takt

Personenbezogene Daten?

Zweck-Definition
- Heizkostenabrechnung
- Effizienzsteuerung Zentralheizung
- Vergleichsübersicht für Mieter

Rechtsgrundlage(n)
- Vertrag mit Mieter (ggf. i.V.m. HKVO)
- Berechtigtes Interesse
- Einwilligung

Grundsätze
- Erforderlichkeit
- Minimierung
- Speicherbegrenzung

Erforderlichkeit
- Jahreswerte für Abrechnung
- unterjährige Verbrauchs-informationen/Stichtagswerte
- 15-Minuten-Werte?

Minimierung
- Anonymisierung durch Aggregation von Rohdaten (Entfernung des Personenbezugs)

Speicherbegrenzung
- Löschfristen für personenbezogene Daten (bspw. 24h/3 Jahre)

Usecase 2: Zentrale Komponenten

datenschutz by migosens

Erfassung Kesseltemperatur

Erfassung Vor- und Rücklauftemperatur

Personenbezogene Daten?

Anwendungsbereich Datenschutzrecht

- bei mehr als 5 Einheiten nicht gegeben

Rechtsgrundlage(n)

- nicht erforderlich, da keine personenbezogenen Daten

Usecase 3: Luftgütemessung

Erfassung Luftfeuchtigkeit und Temperatur in Wohneinheit

Personenbezogene Daten?

Zweck-Definition

- Unterstützung der Mieter bei richtigem Lüften
- Incentivierung von effizientem Heizen

Rechtsgrundlage(n)

- Vertrag mit Mieter
- Einwilligung (Freiwilligkeit sicherstellen!)

Grundsätze

- Erforderlichkeit
- Minimierung
- Speicherbegrenzung

Erforderlichkeit

- Zeitliche Entwicklung über definierten Zeitraum

Minimierung

- Anonymisierung durch Aggregation von Rohdaten (Entfernung des Personenbezugs)

Speicherbegrenzung

- Löschfristen für personenbezogene Daten (bspw. 90 Tage)

Kontakt und weitere Informationsangebote

datenschutz by migosens

migosens

migosens GmbH
Wiesenstr. 35
45473 Mülheim an der Ruhr

Tel. 0208 / 99395110

office@migosens.de

@DS_TALK

datenschutztalk_podcast

linkedin.com/company/migosensgmbh/

Allgemeine Informationen

Bitkom e.V.
https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/index.jsp

Der Datenschutz Talk Podcast
https://www.migosens.de/podcast/

migosens YouTube Channel
https://www.youtube.com/channel/UCyJ2BKkK5qNnNZuTaAi1lkQ

Infos zu Datenschutz bei Gebäudekonnektivität

Urteil LG Dortmund 9 S 1/14
https://openjur.de/u/762235.html

Vortragsreihe Vodafone
https://immobilienwirtschaft.vodafone.de/webinare.html

Auf Anfrage (gk@unitymedia.de): Orientierungshilfe „Datenschutz im Kontext Gebäudekonnektivität 4.0“