Kundeninformation "Verarbeitungsverzeichnis und die DSGVO"

id newmedia KnowHow - für *Sie ...*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

Seit der DSGVO benötigt jedes Unternehmen im Netz ein sogenanntes "Verarbeitungsverzeichnis".

Bild : animationfactory

In diesem Verzeichnis müssen Sie alle Ihre Verarbeitungsvorgänge auflisten :

Woher kommen die Kundendaten in Ihrem Unternehmen ?
Wo gehen diese Daten hin ?
Wie lange werden Daten gespeichert ?
Was passiert mit Daten, wenn man sie nicht mehr benötigt ?

 Stand Februar 2021

Was ist ein Verarbeitungsverzeichnis ?

Ein Verzeichnis von Verarbeitungstätigkeiten ist eine durch das europäische Datenschutzrecht vorgeschriebene Auflistung aller Verarbeitungstätigkeiten personenbezogener Daten. Der Begriff wurde durch die Verordnung (EU) 2016/679, Datenschutz-Grundverordnung (DSGVO) eingeführt. Die frühere Bezeichnung im deutschen Datenschutzrecht lautete Verfahrensverzeichnis. Regelungen zum Verzeichnis über Verarbeitungstätigkeiten finden sich in Artikel 30 der DSGVO und ggf. ergänzende Regelungen in den nationalen Datenschutzgesetzen der EU-Mitgliedsstaaten.

Die EU-Datenschutz-Grundverordnung (DSGVO) schreibt also vor, dass jeder Verantwortliche, der personenbezogene Daten verarbeitet, seine Verarbeitungsvorgänge in einem ausführlichen "Verzeichnis der Verarbeitungstätigkeiten" dokumentieren muss.

Bild : animationfactory

Personenbezogene Daten sind zum Beispiel:

- Bestelldaten von Kunden (siehe auch GOBS)
- Namen und Anschrift des Kunden
- die email-Adresse, z. B. für einen Newsletter
- die IP-Adresse und die URL (z. B. www.id-newmedia.de)

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 12: Einzelhändler – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Bekleidungshaus Huber
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: info@modehuber-fallstadt.de
Web: www.modehuber-fallstadt.de

Inhaber: Gerhard Huber, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über Buchhaltungsbüro)	Hans Klausen 0981/123456-1 hans@ modehuber-fallstadt.de	01.01.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer...	Buchhaltungs-büro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber-fallstadt.de	19.03.2018	Unternehmens-darstellung	• Kunden • Webseitenbesucher	• IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept
Kundenkarten-verwaltung	Marie Greiner 0981/123456-3 marie@ modehuber-fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	• Stammdaten der Kunden • Kaufhistorien	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber-fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	• Stammdaten der Kunden • Zahlungsdaten (Bank-verbindung)	Zahlungsdienst-leister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@ modehuber-fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	• Bestandskunden • potenzielle Neukunden	• Postadressen der Kunden	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Welche Unternehmen müssen ein Verzeichnis von Verarbeitungstätigkeiten erstellen ?

Nach Prof. Dr. Anne Riechert / Stiftung Datenschutz müssen in der Regel alle Unternehmen als Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen.

Artikel 30 Absatz 5 DSGVO beschränkt diese Pflicht unter anderem auf Unternehmen mit einer Größe ab 250 Mitarbeitern [1].

[1] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (C (2003) 1422) (ABl. L 124 vom 20.5.2003, S. 36).

Dies gilt jedoch nicht bei einer regelmäßigen Verarbeitung von Daten.

Letzteres kann stets dann in Betracht kommen, wenn beim Verantwortlichen Mitarbeiter beschäftigt sind und deren Daten verarbeitet werden (Personaldaten).

Kein Verzeichnis von Verarbeitungstätigkeiten müssen nach Art. 30 Abs. 5 DSGVO Verantwortliche und Auftragsverarbeiter mit weniger als 250 Mitarbeitern führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen folgender personenbezogener Daten durch :

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (z. B. Bonitätsscoringverfahren, Betrugspräventionsverfahren)

- oder besondere Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (Religionsdaten, Gesundheitsdaten, biometrische Daten zur eindeutigen Identifizierung etc.)

- oder über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO betreffen

- oder nicht nur gelegentlich erfolgen (alle sonstigen Verarbeitungen, z. B. Lohnabrechnungen, Kundendatenverwaltung, IT-/Internet-/email-Protokollierung, Schulnoten).

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist.

Wegen der regelmäßig erfolgenden Lohnabrechnungen werden damit kaum Unternehmen von der Pflicht eines solchen Verzeichnisses generell befreit sein; allenfalls Unternehmen, die diese Tätigkeiten komplett durch einen Steuerberater erledigen lassen sowie eventuell kleinere Vereine.

In diesem Zusammenhang sei darauf hingewiesen, dass das Bayerische Landesamt für Datenschutzaufsicht bereits Handreichungen veröffentlicht hat, die sich auf kleine Unternehmen fokussieren.

Das Verzeichnis aller Verarbeitungstätigkeiten bedarf der Schriftform. Es kann auch digital geführt werden. Mindestangaben sind :

- Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation unter Nennung des Landes oder der Organisation;

sowie wenn möglich

- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1. DSGVO (TOMs).

In Deutschland werden diese Vorgaben in § 70 Bundesdatenschutzgesetz konkretisiert.

Neben den Verantwortlichen sind auch Auftragsverarbeiter, d. h. natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten, zur Führung des Verzeichnisses über Verarbeitungstätigkeiten verpflichtet. Deren Verzeichnis muss zusätzlich den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter enthalten.

Wer benötigt ein Verarbeitungsverzeichnis ?

Fast jeder Unternehmer – und sei er noch so klein - muss nach der DSGVO ein ausführliches Verarbeitungsverzeichnis führen. Für ganz kleine Unternehmen gibt es zwar Ausnahmen.

Aber : diese Ausnahmen greifen nur, wenn die personenbezogenen Daten „nicht nur gelegentlich“ verarbeitet werden. Leider gibt es keine klare Definition in der juristischen Literatur darüber, was "nicht nur gelegentlich" bedeutet. Jeder Unternehmer sollte diese Dokumentationspflicht also ernst nehmen. Das Verzeichnis kann nicht nur eine gesetzliche Pflicht sein, Sie können es auch als Marketinginstrument zur Kundenbindung nutzen.

Die Aufsichtsbehörde wird Sie bei jeder Prüfung oder Beschwerde zuerst nach diesem Verzeichnis fragen. Ein gutes Verarbeitungsverzeichnis ist also eine rechtliche Pflicht und das "datenschutzrechtliche Aushängeschild" für jedes Unternehmen. Die Verantwortlichen, deren Auftragsverarbeiter sowie deren Vertreter sind verpflichtet, ihr Verzeichnis von Verarbeitungstätigkeiten auf Verlangen der Aufsichtsbehörde zur Verfügung zu stellen.

Bei Verstößen gegen die DSGVO sieht Art. 83 DSGVO Bußgelder vor, so auch bei Verletzung der Verpflichtungen nach Art. 30. Der mögliche Bußgeldrahmen beläuft sich hierbei auf bis zu 10 Millionen Euro oder 2 % des Jahresumsatzes im Vorjahr des Verstoßes.

Welchen Inhalt hat ein Verarbeitungsverzeichnis ?

Für ein DSGVO-konformes Verarbeitungsverzeichnis müssen Sie und Ihre Mitarbeiter sich als Erstes darüber im Klaren sein, welche Angaben in diesem Verzeichnis überhaupt gemacht werden müssen.

Wichtig

Sie müssen nicht alle einzelnen Kundendaten in das Verzeichnis übernehmen. Es geht um die Datenschutz-Vorgänge und Datenkategorien an sich, bei denen Sie personenbezogene Daten speichern oder verarbeiten. Bei den meisten Unternehmen handelt es sich um gängige Geschäftsprozesse, die Sie relativ einfach in ein Verarbeitungsverzeichnis übertragen können.

Wer ist für das Verarbeitungsverzeichnis verantwortlich ?

Verantwortlich für das Verarbeitungsverzeichnis ist der Unternehmer bzw. der Geschäftsführer des Unternehmens. Sie müssen im Rahmen der Dokumentationspflicht der DSGVO sämtliche Verarbeitungstätigkeiten dokumentieren. Nur so sind Sie bei Prüfungen der Aufsichtsbehörden auf der sicheren Seite.

Wichtig

Das gilt nicht nur für die Daten in der Beziehung Unternehmer - Kunde. Sondern auch für Daten, die zum Beispiel im Rahmen der Auftragsverarbeitung
(früher: Auftragsdatenverarbeitung) anfallen.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DSGVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur **ein** Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen.

So müssen bspw. auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1 DSGVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1 DSGVO) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DSGVO) durch entsprechende Dokumentationen nachgewiesen werden.

Vor diesem Hintergrund bietet es sich an, das Verzeichnis sinnvollerweise auch folgendermaßen einzusetzen bzw. zu verwenden :

- für eine Festlegung der Verarbeitungszwecke nach Art. 5 Abs. 1 lit. b DSGVO;
- für Zwecke der Rechenschafts- und Dokumentationspflicht, Art. 5 Abs. 2, Art. 24 DSGVO;
  - als Nachweis der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a DSGVO;
  - als Nachweis der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO;
  - als Nachweis der Richtigkeit und Aktualität der Daten nach Art. 5 Abs. 1 lit. d DSGVO;
- als geeignete Maßnahme zur Erfüllung der Betroffenenrechte nach Art. 12 Abs. 1 DSGVO;
- zur Schaffung und als Nachweis geeigneter technischer und organisatorischer Maßnahmen nach Art. 24 Abs. 1 und Art. 32 DSGVO;
- zur Prüfung, ob eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO erfolgen muss;
- als Basis für die Aufgabenerfüllung des Datenschutzbeauftragten nach Art. 39 DSGVO.

Die Verzeichnisse sind gemäß Art. 30 Abs. 3 DSGVO schriftlich zu führen.

Dies kann auch in einem elektronischen Format erfolgen.

Bild : animationfactory

Die Aufsichtsbehörde kann das Format der Vorlage (schriftlich in Papierform oder elektronisch in Textform) eigenständig festlegen und daher auch bei einem im elektronischen Format geführten Verzeichnis den Ausdruck verlangen (§ 3a VwVfG). Maßstab sind die Verhältnismäßigkeit und Erforderlichkeit für die jeweils verfolgten aufsichtlichen Zwecke (z. B. nur der erforderliche Teil wird ausgedruckt).

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 6: WEG-Verwaltung – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Hausverwaltung Jasmin Haberecker
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@habereckerhv.de
Web: www.habereckerhv.de

Geschäftsführerin: Kerstin Haberecker, geb. 03.12.1974

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Abrechnung für Eigentümerge-meinschaften	Kerstin Haberecker 0981/123456-0 kerstin@habereckerhv.de	02.03.2018	Abrechnung als Verwalter gemäß § 28 Abs. 3 WEG	Wohnungs-eigentümer	• Namen, Kontaktdaten • Bankverbindungsdaten • (anteilige) Einnahmen und Ausgaben • Vorschüsse, Beitragsleistungen, Rückstände • Heiz- u. Warmwasserkosten	Eigentümer in der betr. Gemein-schaft	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Wirtschaftsplan für Eigentümer-gemeinschaften	Kerstin Haberecker 0981/123456-0 kerstin@habereckerhv.de	02.03.2018	Aufstellung Wirtschaftsplan als Verwalter gemäß § 28 Abs. 1 WEG	Wohnungs-eigentümer	• anteilige Verpflichtungen (Kosten- u. Lasten) • anteilige Beitragsleistung zur Instandhaltungsrücklage • ggf. anteilige Sonderumlagen	Eigentümer in der betr. Gemein-schaft	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist	Siehe IT-Sicherheits-konzept
Management d. Eigentümer-versammlungen	Kerstin Haberecker 0981/123456-0 kerstin@habereckerhv.de	02.03.2018	Vorbereitung u. Dokumentation der Eigentümerversammlungen, Beschlusssammlung	Wohnungs-eigentümer	• Namen, Kontaktdaten • Protokolle von Eigentümerversammlungen inkl. Äußerungen u. Abstimmungsverhalten	Eigentümer in der betr. Gemein-schaft	...	...	...
Erfassung u. Abrechnung d. Heiz-/Warm-wasserkosten	Tim Scheuerlein 0981/123456-2 tim@habereckerhv.de	02.03.2018	Erfassung und Verteilung der Heiz- u. Warmwasserkosten	Wohnungs-eigentümer	• Verbrauchswerte für Heizung und Warmwasser • anteilige Kostentragungs-pflichten für die Eigentümer	externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist	Siehe IT-Sicherheits-konzept
Personal-verwaltung	Jasmin Haberecker 0981/123456-1 jasmin@habereckerhv.de	02.03.2018	• Personaladministration • Personalführung • Arbeitszeitverwaltung	Beschäftigte	• Name, Adressen • Zeitwirtschaftsdaten • Daten zur Arbeitsleistung • Leistungsbeurteilung	Keine	Keine	in der Regel ca. 3 Jahre nach Ausscheiden	Siehe IT-Sicherheits-konzept
Lohn-abrechnung (Steuerberater)	Jasmin Haberecker 0981/123456-1 jasmin@habereckerhv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name, Geburtsdatum • Adresse • Bankverbindungsdaten ...	Steuer-berater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Uwe Wiedemann 0981/123456-0 uwe@habereckerhv.de	28.02.2018	Außendarstellung	Webseiten-besucher	IP-Adressen	externer Dienstleister	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheits-konzept + HTTPS
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Wir beraten Sie gerne …