

Daniela Frank

DSGVO einfach umsetzen?

Mach's wie Henry!

Die Schritt-für-Schritt-Anleitung
zur praktischen Umsetzung des Datenschutzes

ISBN: 978-3-00-076644-2

© 2023 Machs wie Henry GmbH. Alle Rechte vorbehalten.

Dieses Werk ist einschließlich aller Teile urheberrechtlich geschützt. Nachdruck oder Reproduktion in irgendeiner Form ist ohne Zustimmung der Machs wie Henry GmbH unzulässig und strafbar.

www.machs-wie-henry.de

Vorwort

Liebe Leserinnen und Leser,

mit großer Freude präsentiere ich Ihnen diese Schritt-für-Schritt-Anleitung zur Umsetzung der Datenschutzgrundverordnung (DSGVO). Die DSGVO, die im Mai 2018 in Kraft trat, markiert einen wichtigen Meilenstein in der modernen Datenschutzlandschaft. Sie legt klare und umfassende Richtlinien fest, die den Schutz personenbezogener Daten gewährleisten und das Vertrauen in die digitale Welt stärken sollen.

In der heutigen digitalen Ära sind Daten zu einem unverzichtbaren Rohstoff geworden, der Wirtschaft und Gesellschaft gleichermaßen antreibt. Doch dieser wertvolle Rohstoff birgt auch eine Verantwortung, nämlich sicherzustellen, dass personenbezogene Daten mit größter Sorgfalt und Integrität behandelt werden. Unternehmen stehen daher vor der Herausforderung, die Bestimmungen der DSGVO in ihrem täglichen Umgang mit Daten zu berücksichtigen.

In diesem Buch liegt mein besonderes Augenmerk auf einer Verarbeitungstätigkeit als exemplarischem Beispiel. Gemeinsam werden wir die Schritte durchgehen, die erforderlich sind, um die DSGVO erfolgreich umzusetzen und den Anforderungen gerecht zu werden. Dabei wird der Fokus nicht nur auf den rechtlichen Aspekten liegen, sondern auch auf praxisnahen Lösungsansätzen.

Der Ratgeber soll Ihnen als wertvolle Hilfestellung dienen, ganz gleich, ob Sie ein Unternehmen leiten oder als Mitarbeiter für den Datenschutz in Ihrem Unternehmen zuständig sind. Die DSGVO mag zunächst komplex erscheinen, aber mit dem richtigen Verständnis und der richtigen Herangehensweise können Sie die Datenschutzanforderungen in den Arbeitsalltag integrieren, ohne dass dies zu einer unüberwindbaren Hürde wird.

Es ist mir ein Anliegen, dieses Buch nicht nur informativ, sondern auch praxisnah und verständlich zu gestalten. Die DSGVO sollte nicht als bürokratisches Hindernis betrachtet werden, sondern als wertvolle Möglichkeit, das

Vertrauen Ihrer Kunden und Mitarbeiter zu gewinnen und langfristige Geschäftsbeziehungen aufzubauen.

Ich möchte mich herzlich bei all denjenigen bedanken, die mich bei der Erstellung dieses Ratgebers unterstützt haben. Mein Dank gilt auch Ihnen, liebe Leserinnen und Leser, die Sie sich die Zeit nehmen, dieses Buch zu lesen. Ich hoffe aufrichtig, dass es Ihnen dabei hilft, die DSGVO besser zu verstehen, erfolgreich in die Praxis umzusetzen und den einen oder anderen „Aha-Moment“ zu erleben.

Datenschutz ist nicht nur ein rechtliches Gebot, sondern auch ein ethisches Prinzip. Wenn wir uns gemeinsam für den Schutz personenbezogener Daten einsetzen, können wir eine vertrauenswürdige und nachhaltige digitale Welt gestalten.

Meine lieben Leserinnen: Um die Lesbarkeit dieses Buches zu erleichtern, habe ich mich entschieden, bei Personenbezeichnungen nur die männliche Form zu verwenden. Ich hoffe, dass dies auch in Ihrem Interesse ist und Sie sich gleichwohl angesprochen fühlen.

Viel Vergnügen beim Lesen!

Daniela Frank

Heiligenhaus, Oktober 2023

Einleitung.....	1
1. Schritt: Anwendungsbereich der DSGVO	3
2. Schritt: Dokumentation des Ablaufs	7
3. Schritt: Zweckbestimmung.....	9
4. Schritt: Betroffene Person	11
5. Schritt: Personenbezogene Daten	13
6. Schritt: Rechtsgrundlage	23
7. Schritt: Herkunft der Daten	46
8. Schritt: Empfänger der Daten.....	50
9. Schritt: Eingesetzte Anwendungen und Systeme	70
10. Schritt: Automatisierte Entscheidungsfindung einschließlich Profiling.....	78
11. Schritt: Bereitstellung der Daten	87
12. Schritt: Löschfristen und Aufbewahrungsdauer.....	89
13. Schritt: Technische und organisatorische Maßnahmen	121
14. Schritt: Informationspflichten	151
Datenschutzverletzungen.....	167
Betroffenenrechte.....	177
Die Webseite	198
Mitarbeiter schulen und sensibilisieren.....	211
Sachverhalt prüfen und dokumentieren	213
Bestandsaufnahme	217
Regelmäßige Überprüfung.....	220
Weiterführende Informationen.....	222
Abbildungsverzeichnis.....	229
Stichwortverzeichnis	234

Einleitung

Gestatten Sie, mein Name ist Henry, und ich werde Ihnen in diesem Buch eine effektive und zeitsparende Methode zur Umsetzung des Datenschutzes darstellen. Woher ich das weiß? Ich habe selbst ein Unternehmen und habe es geschafft, den Datenschutz vollständig und effektiv umzusetzen. War es einfach? Ganz und gar nicht! Rückblickend habe ich unglaublich viele zeitraubende Fehler gemacht und war mehr als einmal kurz davor, frustriert aufzugeben. Hätten diese Fehler vermieden werden können? Auf jeden Fall! Nämlich dann, wenn mir die Zusammenhänge der Vorgaben der Datenschutzgrundverordnung („DSGVO“) und deren Sinn von Anfang an klar gewesen wären. Diese rechtzeitige Erkenntnis war mir aber leider nicht vergönnt. Bei mir „fiel der Groschen“ erst, als ich den Datenschutz über viele zeitraubende Umwege endlich vollständig umgesetzt hatte.

Um Sie vor den gleichen zeitraubenden Fehlern zu bewahren, werde ich mit Ihnen nun Schritt für Schritt eine Verarbeitungstätigkeit erstellen. Mit dieser Vorgehensweise werden Sie am Ende alle Anforderungen der DSGVO kennengelernt und das Prinzip verstanden haben. Eine Verarbeitungstätigkeit ist ein Verarbeitungsvorgang, bei dem Daten von betroffenen Personen verarbeitet werden. Wenn Sie also eine Bestellung abwickeln, den Urlaub Ihrer Mitarbeiter verwalten oder Zahlungen vornehmen, werden personenbezogene Daten von Kunden oder Mitarbeitern verarbeitet, die unter die DSGVO fallen und nur unter bestimmten Voraussetzungen verarbeitet werden dürfen. Unabhängig davon, welchen Verarbeitungsvorgang Sie als Verarbeitungstätigkeit erstellen möchten, ist die Vorgehensweise immer dieselbe. Die einzelne Verarbeitungstätigkeit ist dabei der Grundstein für eine datenschutzkonforme Verarbeitung und Ihr Verarbeitungsverzeichnis gem. Art. 30 DSGVO, in dem alle Verarbeitungstätigkeiten erfasst werden, das „Herz“ Ihres Datenschutzes. Das klingt vielleicht etwas hochtrabend, aber am Ende werden Sie feststellen, dass es keinen treffenderen Ausdruck für die Funktion Ihres Verarbeitungsverzeichnisses gibt. Welche Voraussetzungen Sie beachten müssen, werden wir Schritt für Schritt anhand der Verarbeitungstätigkeit „Visitenkarten“ durchgehen. Dabei geht es um die betrieblichen Visitenkarten, die wir für unsere Mitarbeiter erstellen und verwalten möchten. Bitte beachten Sie, dass ich Ihnen eine Methode an die Hand geben möchte, die

nicht alle Besonderheiten berücksichtigen kann. Die Lektüre der Artikel der DSGVO bzw. der Paragraphen des BDSG sowie das Hinzuziehen weiterführender Informationen zu einzelnen Themen bleiben daher unerlässlich. Nach der Lektüre dieses Buches werden Sie aber ein solches Verständnis für die Anforderungen entwickelt haben, dass Sie nach dem Lesen der Normen der DSGVO oder den Orientierungshilfen der Aufsichtsbehörden mehr als nur „Bahnhof“ verstehen werden.

Am Ende können Sie den Datenschutz so in Ihrem Unternehmen implementieren, dass Ihre Mitarbeiter den Datenschutz umsetzen, ohne zu merken, dass sie den Datenschutz umsetzen. Das verstehen Sie nicht? Ich verspreche Ihnen: Wenn Sie das Buch komplett gelesen haben, wird auch bei Ihnen der „Groschen fallen“...

1. Schritt: Anwendungsbereich der DSGVO

Bevor wir uns die Mühe machen, eine Verarbeitungstätigkeit zu erstellen, prüfen wir zunächst, ob wir die DSGVO überhaupt beachten müssen. Spoiler: In 99 % der Fälle wird das der Fall sein.

Da wir unseren Sitz in Deutschland und damit in der EU haben, findet die DSGVO auf jeden Fall in „räumlicher“ Hinsicht Anwendung.

Als nächstes müssen wir prüfen, ob sie auch in „sachlicher“ Hinsicht Anwendung findet: Was wollen wir mit den Daten machen? Wir wollen Visitenkarten erstellen und verwalten. Also werden wir die Daten zumindest erfassen, speichern und wahrscheinlich auch übermitteln. Und wie machen wir das? Ziemlich sicher mit einem Computer. Damit haben wir schon einmal eine automatisierte Verarbeitung. Damit die DSGVO auch greift, müssen die Daten aber auch personenbezogen sein. Auf Visitenkarten stehen in der Regel der Name und die Kontaktdaten eines Mitarbeiters. Ohne an dieser Stelle näher auf die Definition personenbezogener Daten eingehen zu müssen, liegt es auf der Hand, dass auch diese Daten personenbezogen sind. Damit ist die DSGVO auch in „sachlicher“ Hinsicht zu beachten.

Prima! Wenn wir Visitenkarten für unsere Mitarbeiter erstellen wollen, müssen wir uns an die Vorgaben der DSGVO halten. Also los...

Machen Sie's wie Henry!

Nicht immer - aber meistens - ist die DSGVO zu berücksichtigen, wenn Daten verarbeitet werden. Ob die DSGVO anwendbar ist, bestimmt sich zunächst in räumlicher und sachlicher Hinsicht:

Räumlicher Anwendungsbereich

Art. 3 DSGVO legt fest, wann der „räumliche“ Anwendungsbereich eröffnet ist:

1. Wenn ein Unternehmen oder eine Organisation ihren Sitz oder eine Niederlassung (z. B. ein Büro oder eine Geschäftsstelle) in der EU hat oder von einem Dienstleister in der EU unterstützt wird, und im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeitet, gilt die

- DSGVO unabhängig davon, ob die Datenverarbeitung in der EU stattfindet oder nicht.
2. Wenn ein Unternehmen oder eine Organisation keinen Sitz in der EU hat, aber personenbezogene Daten von Personen verarbeitet, die sich in der EU aufhalten, gilt die DSGVO, wenn diese Datenverarbeitung im Zusammenhang mit folgenden Situationen steht:
 - a. Das Unternehmen bietet Waren oder Dienstleistungen für Personen in der EU an, unabhängig davon, ob diese Personen dafür bezahlen oder nicht.
 - b. Das Unternehmen beobachtet das Verhalten von Personen in der EU und dieses Verhalten findet auch in der EU statt.
 3. Schließlich gilt die DSGVO auch für die Verarbeitung personenbezogener Daten durch ein Unternehmen oder eine Organisation außerhalb der EU, wenn diese Verarbeitung an einem Ort erfolgt, der aufgrund Völkerrechts dem Recht eines EU-Mitgliedstaats unterliegt.

Zusammengefasst: Jeder „Verantwortliche“, der seinen Sitz in der EU hat und personenbezogene Daten verarbeitet oder personenbezogene Daten von Bürgern verarbeitet, die sich in der EU aufhalten, muss die DSGVO beachten.

Ein „Verantwortlicher“ ist nach Art. 4 Nr. 7 DSGVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Eine „Person“ wird also dann zum Verantwortlichen, wenn sie darüber entscheidet, wie („Mittel“) und wofür („Zweck“) personenbezogene Daten verarbeitet werden. In der Regel ist dies also der Inhaber eines Unternehmens oder eine GmbH, vertreten durch ihren Geschäftsführer. Damit sind z. B. Mitarbeiter grundsätzlich keine Verantwortlichen, solange sie die Daten nach Weisung des Verantwortlichen verarbeiten. Entscheidet sich aber ein Mitarbeiter, die Daten des Verantwortlichen für eigene Zwecke zu nutzen (sog. „Mitarbeiterexzess“), wird auch er zum Verantwortlichen. Das ist schnell passiert. Es reicht schon aus, wenn ein Mitarbeiter einen Kunden zu privaten Zwecken kontaktiert oder die Datenbank des Unternehmens oder der Behörde zu privaten Zwecken durchsucht. Schließlich können auch Privatpersonen schnell zu Verantwortlichen

werden, wenn sie beispielsweise eine „Dashcam“ in ihrem Privatfahrzeug installiert haben.

Sachlicher Anwendungsbereich

Neben dem räumlichen Anwendungsbereich gibt es nach Art. 2 DSGVO auch einen „sachlichen Anwendungsbereich“. Danach gilt die DSGVO „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“. Die Voraussetzungen sind also

- Verarbeitung,
- ganz oder teilweise automatisiert oder nichtautomatisiert und
- personenbezogene Daten.

Verarbeitung

Der Begriff „Verarbeitung“ ist in Art. 4 Nr. 2 DSGVO definiert. Eine Verarbeitung liegt immer dann vor, wenn Sie Daten ...

- erheben,
- erfassen,
- organisieren,
- ordnen,
- speichern,
- anpassen oder verändern,
- auslesen,
- abfragen,
- verwenden,
- offenlegen durch Übermitteln, Verbreiten oder eine andere Form der Bereitstellung,
- abgleichen oder verknüpfen,
- einschränken,
- löschen oder vernichten,
- ...

Im Grunde ist alles, was Sie mit Daten machen können, eine Verarbeitung im Sinne der DSGVO. Auch wenn Sie Daten nur speichern, ohne etwas damit zu tun, handelt es sich um eine Verarbeitung.

Ganz oder teilweise automatisiert oder nichtautomatisiert

Eine automatisierte Verarbeitung liegt vor, wenn Daten mit einem Computer, Smartphone oder Tablet verarbeitet werden. Auch der Einsatz von Kameras, Webcams, Scannern oder Kopierern stellt eine automatisierte Verarbeitung dar.

Papierakten oder handschriftliche Aufzeichnungen stellen dagegen eine nichtautomatisierte Verarbeitung dar. Sie fallen nur dann in den Anwendungsbereich der DSGVO, wenn sie in einem „Dateisystem“ gespeichert sind oder gespeichert werden sollen. Ein Dateisystem ist nach Art. 4 Nr. 6 DSGVO „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird“. Eine Schublade, in die Sie Visitenkarten werfen, ist also kein Dateisystem und fällt nicht unter die DSGVO. Sobald Sie die Visitenkarten aber beispielsweise alphabetisch sortieren, greift die DSGVO wieder. Erst recht, wenn Sie die Daten der Visitenkarten in Ihrer Kontaktdatenbank auf dem Computer erfassen.

Personenbezogene Daten

Schließlich müssen die Daten auch personenbezogen sein und sich auf eine „natürliche“ identifizierte oder identifizierbare Person beziehen. Ist das nicht der Fall, dürfen Sie die Daten nach Lust und Laune verarbeiten, ohne die Vorgaben der DSGVO beachten zu müssen. Wann genau Daten personenbezogen sind, wird im Kapitel „5. Schritt: Personenbezogene Daten“ vertieft behandelt.

2. Schritt: Dokumentation des Ablaufs

Nun, da wir herausgefunden haben, dass wir die Anforderungen der DSGVO erfüllen müssen, wenn wir Visitenkarten für unsere Mitarbeiter erstellen und verwalten wollen, müssen wir eine Verarbeitungstätigkeit erstellen.

Bevor wir jedoch mit der Erstellung unserer Verarbeitungstätigkeit beginnen, nehmen wir uns die Zeit, den Ablauf des Verarbeitungsvorgangs zu dokumentieren oder zumindest zu skizzieren. Dies hängt davon ab, wie viel wir bereits über den Ablauf wissen:

- Für die Erstellung und Verwaltung von Visitenkarten ist Beate Müller (Verwaltung) zuständig.
- Über neue Mitarbeiter wird sie von der Personalabteilung informiert.
- Die Daten eines neuen Mitarbeiters erfasst sie in der Vorlage „Vorlage_Visitenkarten.docx“.
- Die Vorlage speichert sie in dem Personalordner des Mitarbeiters.
- Danach sendet sie den Entwurf per E-Mail an den Mitarbeiter zur Info sowie dem Abteilungsleiter der Verwaltung Emil Fuchs zur Freigabe.
- Nach Freigabe erstellt sie aus dem Word-Dokument ein PDF.
- Die Visitenkarten werden durch die Firma Visitenkartendruckerei GmbH gedruckt.
- Für die Beauftragung wird das erstellte PDF über den Account hochgeladen und die Bestellung mit der festgelegten Formatierung ausgelöst.
- Die Zugangsdaten lauten:
Benutzername: beate.mueller@henry-muster.de
Passwort: 12Passwort!
- Die E-Mail mit der Auftragsbestätigung sowie die Rechnung wird von Frau Müller per E-Mail an Anna Harting in die Buchhaltung weitergeleitet.
- Die gedruckten Visitenkarten werden von Frau Müller geprüft und an den Mitarbeiter übergeben.

Abbildung 1: Ablauf

Sie sind es nicht gewohnt, jeden Vorgang zu dokumentieren? Damit sind Sie nicht allein. Auch ich habe das immer für Zeitverschwendung gehalten. Schließlich wussten meine geschätzten Mitarbeiter auch so, was sie zu tun hatten. Ich kann Ihnen aber versprechen, dass Sie am Ende froh sein werden, sich die Mühe gemacht zu haben, auch wenn Sie jetzt wahrscheinlich noch nicht ganz klar ist, wie die Erstellung eines zeitaufwendigen Ablaufs zu einer zeitsparenden Umsetzung der DSGVO führen soll. Der dokumentierte Ablauf ist später ein elementarer Baustein für die Einhaltung des Datenschutzes im Arbeitsalltag.

Machen Sie's wie Henry!

Die Erstellung eines detaillierten Ablaufs der Verarbeitungstätigkeiten ist zwar keine Anforderung der DSGVO, aber Sie schlagen damit zwei Fliegen mit einer Klappe:

- Dem Ablauf können Sie bereits viele Pflichtangaben für Ihr Verarbeitungsverzeichnis entnehmen.
- Mit jedem Ablauf erstellen Sie automatisch auch ein umfassendes Organisationshandbuch.
- Der Ablauf ist später entscheidend für eine effektive datenschutzkonforme Verarbeitung.

Auch wenn Sie sich jetzt nur schwer vorstellen können, wie sich dieser vermeintliche Mehraufwand später auszahlen soll, werden Sie am Ende feststellen, dass er Ihnen gute Dienste erweisen wird.

3. Schritt: Zweckbestimmung

Nachdem wir nun den gesamten Ablauf der Verarbeitungstätigkeit „Visitenkarten“ dokumentiert haben, kommen wir zur ersten Anforderung der DSGVO und bestimmen den Zweck unserer Verarbeitungstätigkeit. Das ist in unserem Beispiel gar nicht so schwer, oder?!

Verarbeitungstätigkeit	Zweck
Visitenkarten	Erstellung und Verwaltung von betrieblichen Visitenkarten

Abbildung 2: Zweckbestimmung im Verarbeitungsverzeichnis

Nun beschreiben wir in wenigen Sätzen, worum es sich bei dieser Verarbeitungstätigkeit genau handelt. Wir stellen uns einfach vor, dass uns ein Mitarbeiter gefragt hat, was denn genau gemacht wird:

Zweckbeschreibung
Wenn Sie im Bereich der Kundengewinnung tätig sind, erstellen und verwalten wir für Sie Visitenkarten, die Sie bei Bedarf weitergeben können. Die Visitenkarten enthalten üblicherweise Ihren Vor- und Nachnamen, Ihre Position oder Funktion sowie ihre geschäftlichen Kontaktdaten. Um zu gewährleisten, dass alle Visitenkarten unseren Vorgaben entsprechen, werden diese zentral in der Verwaltung aufbewahrt. Wenn Sie das nicht möchten, können Sie Widerspruch einlegen.

Abbildung 3: Zweckbeschreibung im Verarbeitungsverzeichnis

Und schon können wir diese Anforderung mit einem Häkchen versehen.

Machen Sie's wie Henry!

Vor der Prüfung aller weiteren Anforderungen ist zunächst der Zweck zu bestimmen. Dieser ist eine Pflichtangabe im Verarbeitungsverzeichnis (Art. 30 Abs. 1 lit. b) DSGVO) und ergibt sich zudem aus dem „Grundsatz der Zweckbindung“ (Art. 5 Abs. 1 lit. b) DSGVO).

Der sperrige Begriff „Zweck“ kann auch als „Ziel“ der Verarbeitung umschrieben werden, was Ihnen die Zweckbestimmung etwas erleichtern dürfte.

Bei der Zweckbestimmung ist Folgendes zu beachten:

- Sie müssen den Zweck festgelegt haben, bevor Sie mit der Verarbeitung beginnen. Sie dürfen also keine Daten auf Vorrat sammeln, nur für den Fall, dass Sie sie irgendwann einmal brauchen könnten.
- Der Zweck muss „eindeutig“ sein. Das ist er dann, wenn die betroffene Person – in dem obigen Beispiel also der Mitarbeiter – nachvollziehen kann, wofür seine Daten konkret verarbeitet werden. Bei einer weit gefassten Zweckbestimmung wie „Vertriebszwecke“ wäre dies nicht möglich und ist so weit gefasst auch nicht zulässig.
- Manchmal lässt sich der Zweck nicht eindeutig bestimmen, so dass sich der Inhalt der Verarbeitung für die betroffene Person ohne weiteres ergibt. In diesen Fällen kann eine kurze Beschreibung des Zwecks hilfreich sein.
- Der Zweck der Verarbeitung muss „rechtmäßig“, er darf also nicht verboten sein.

Die Zweckbestimmung legt quasi den Rahmen fest, in dem Sie die dafür erforderlichen personenbezogenen Daten der betroffenen Personen verarbeiten dürfen. Das bedeutet aber auch, dass Sie die für einen bestimmten Zweck erhobenen Daten nicht ohne weiteres für andere Zwecke weiterverarbeiten dürfen.

Die Zweckbeschreibung ist keine direkte Anforderung der DSGVO. Sie kann aber später im Rahmen Ihrer Informationspflichten und der Erfüllung des „Grundsatzes der Transparenz“ sehr nützlich sein.

4. Schritt: Betroffene Person

Im nächsten Schritt müssen wir jetzt dokumentieren, wessen Daten wir verarbeiten. Das ist in unserem Fall schnell erledigt:

Betroffene Personen	
•	Mitarbeiter (intern)
•	Mitarbeiter des Dienstleisters

Abbildung 4: Betroffene Personen im Verarbeitungsverzeichnis

Dass wir die Daten unserer eigenen Mitarbeiter verarbeiten, war leicht zu erkennen. Aber haben Sie auch daran gedacht, dass auch die Daten von externen Mitarbeitern verarbeitet werden könnten? In unserem Fall enthält etwa die Rechnung und die Auftragsbestätigung den Namen und die Kontaktdaten eines Mitarbeiters der Druckerei. Vielleicht gibt es aber auch Probleme bei der Auftragsabwicklung und wir müssen mit deren Support per E-Mail kommunizieren? Auch dann müssen wir unweigerlich die Daten von deren Mitarbeitern verarbeiten, die damit für uns zu betroffene Personen werden.

Machen Sie's wie Henry!

Dokumentieren Sie die Kategorien von Personen, deren Daten Sie verarbeiten, da es sich hierbei um eine Pflichtangabe für das Verarbeitungsverzeichnis (Art. 30 Abs. 1 lit. c) DSGVO) handelt.

Wie bereits eingangs erwähnt, muss es sich bei den betroffenen Personen um „natürliche“ Personen handeln, damit die DSGVO Anwendung findet. Die übliche Unterscheidung zwischen „natürlichen“ und „juristischen“ Personen hilft hier jedoch nur bedingt weiter. In den meisten Fällen wird es zwar so sein, dass Daten, die sich auf eine klassische „juristische“ Person wie eine GmbH oder AG beziehen, nicht unter die DSGVO fallen. Bei einer GmbH mit nur einem Gesellschafter kann das aber schon anders aussehen: Wenn Sie Daten über die Vermögensverhältnisse einer GmbH verarbeiten, dann schlagen sich diese Informationen bei einer GmbH mit nur einem Gesellschafter auch direkt auf die Vermögensverhältnisse des Gesellschafters und

damit einer natürlichen Person durch. Eine GmbH ist somit niemals keine „natürliche“ Person.

Schauen Sie also bei „klassischen“ juristischen Personen etwas genauer hin und prüfen Sie, ob es sich nicht doch um eine „natürliche“ Person handeln könnte.

5. Schritt: Personenbezogene Daten

Lassen Sie uns nun zu den personenbezogenen Daten kommen.

Zunächst bestimmen wir alle „Datenarten“, die im Rahmen der Verarbeitungstätigkeit anfallen können. Eine Datenart ist im Wesentlichen eine „Sammlung von Daten“. Dies kann ein Dokument, ein Verzeichnis oder eine Datei sein. Folgende Datenarten fallen bei uns an:

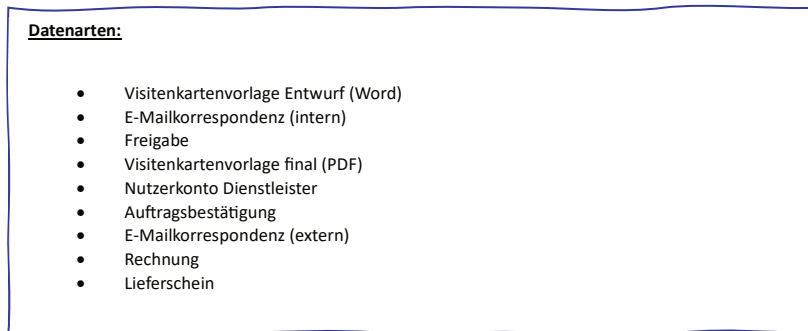


Abbildung 5: Übersicht Datenarten

Um die Übersicht zu erstellen, müssen wir nur einen Blick in unseren Ablauf werfen – da steht das meiste schon drin.

Nun schauen wir uns die Datenarten genauer an und notieren, welche Daten der betroffenen Personen, in unserem Fall also unseres Mitarbeiters und des Mitarbeiters des Dienstleisters, dabei üblicherweise verarbeitet werden können. Lassen Sie sich von der folgenden Übersicht nicht abschrecken – wir werden sie im Laufe des Kapitels noch entschärfen:

Datenarten:

- Visitenkartenvorlage Entwurf (Word)
Mitarbeiter:
Vorname, Name (auch Informationen in Word), Titel, Position, Funktion, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), Erstellungs-, Änderungs- und Druckdatum
- E-Mailkorrespondenz (intern)
Mitarbeiter:
Vorname, Name, Titel, Position, Funktion, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), E-Mailtext, IP-Adresse, Sende- und Empfangszeitpunkt
- Freigabe
Mitarbeiter:
siehe E-Mailkorrespondenz
- Visitenkartenvorlage final (PDF)
Mitarbeiter
siehe Visitenkartenvorlage Entwurf (Word)
- Nutzerkonto Dienstleister
Mitarbeiter
Visitenkartenvorlage Entwurf (Word), Benutzername, Passwort
- Auftragsbestätigung
Mitarbeiter:
Vorname, Nachname, E-Mailadresse (geschäftlich)
Mitarbeiter (extern):
Vorname, Nachname, Titel, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), Unterschrift
- E-Mailkorrespondenz (extern)
Mitarbeiter:
Vorname, Name, Titel, Position, Funktion, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), E-Mailtext, IP-Adresse, Sende- und Empfangszeitpunkt
Mitarbeiter (extern):
Vorname, Name, Titel, Position, Funktion, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), E-Mailtext, IP-Adresse, Sende- und Empfangszeitpunkt
- Rechnung
Mitarbeiter:
Vorname, Nachname, E-Mailadresse (geschäftlich)
Mitarbeiter (extern):
Vorname, Nachname, Titel, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich), Unterschrift
- Lieferschein
Mitarbeiter:
Vorname, Nachname, E-Mailadresse (geschäftlich), Unterschrift
Mitarbeiter (extern):
Vorname, Nachname, Titel, Firma, Anschrift (geschäftlich), Telefon (geschäftlich), E-Mailadresse (geschäftlich)

Abbildung 6: Datenarten mit personenbezogenen Daten

Lassen Sie mich jetzt mal Ihre Gedanken lesen:

„Wir verschicken doch in allen möglichen Bereichen E-Mails. Muss ich jetzt bei jeder Verarbeitungstätigkeit auch diese Daten erfassen?!“

„Und was ist mit Auftragsbestätigungen, Lieferscheinen oder Rechnungen?!“

„Daten von externen Mitarbeitern? Das ist jetzt aber schon etwas übertrieben. Wir korrespondieren doch ständig mit den Mitarbeitern unserer Vertragspartner oder Behörden. Was können wir dafür, wenn die uns ihre Daten mitschicken?!“

Sie haben mit Ihren Überlegungen völlig recht: Das lässt sich erheblich vereinfachen:

Lassen Sie uns mit den Daten zu den externen Mitarbeitern beginnen: Auch wenn wir diese Daten nicht selbst angefordert haben und vielleicht auch gar nicht haben wollen, ändert dies nichts daran, dass wir auch für diese Daten die Anforderungen der DSGVO beachten müssen, da wir sie regelmäßig erhalten, in unserem System speichern und damit verarbeiten. Aus dieser Nummer kommen wir leider nicht heraus. Damit wir aber nicht bei jeder einzelnen Verarbeitungstätigkeit, die wir erstellen, auch die Daten der externen Mitarbeiter berücksichtigen müssen, „lagern“ wir diese Verarbeitung einfach in eine eigene Verarbeitungstätigkeit aus und müssen uns so nur einmal damit befassen. Es spielt dann keine Rolle mehr, in wie vielen Verarbeitungstätigkeiten noch Daten von externen Mitarbeitern verarbeitet werden: Wenn wir dafür eine eigene Verarbeitungstätigkeit erstellt haben, müssen wir diese nicht mehr berücksichtigen. Die neue Verarbeitungstätigkeit könnte dann beispielsweise mit „Verarbeitung Daten von Mitarbeitern des Vertragspartners, Behörden u.a.“ bezeichnet werden.

Gleiches gilt für die Korrespondenz per E-Mail: Wir korrespondieren nahezu mit allen möglichen betroffenen Personen: Mitarbeitern, Kunden oder Interessenten. In jeder E-Mail sind mindestens die E-Mail-Adresse, die IP-Adresse, das Sende- und das Empfangsdatum enthalten. In den meisten Fällen enthalten sie auch den Namen und die Kontaktdaten sowohl des Absenders als auch des Empfängers. Erstellen wir auch hierfür eine eigene Verarbeitungstätigkeit „Kommunikation per E-Mail“, müssen wir auch diese Daten

zukünftig nicht mehr bei jeder Verarbeitungstätigkeit, in der auch per E-Mail kommuniziert wird, berücksichtigen.

Aber aufgepasst: Diese Verarbeitungstätigkeit kann dann nur die Daten enthalten, die regelmäßig bei der E-Mail-Korrespondenz anfallen können. Die Informationen, die im Inhalt einer E-Mail selbst enthalten sind, hängen dann wiederum von der jeweiligen Verarbeitungstätigkeit ab. Handelt es sich bei diesen Informationen um personenbezogene Daten, sind diese wiederum bei der jeweiligen Verarbeitungstätigkeit zu berücksichtigen. Immerhin müssen wir uns dann nicht mehr mit den „Standarddaten“ befassen.

Haben Sie auch das „Erstellungs-, Änderungs- und Druckdatum“ und die „Informationen in Word“ bemerkt? Jedes Dokument, sei es ein Word-Dokument oder eine PDF-Datei, erfasst und speichert in der Regel den Vor- und Nachnamen des Verfassers und der Person, die das Dokument zuletzt geändert hat. Jeder, der die Datei erhält oder Zugriff darauf hat, kann diese Informationen einsehen. Auch wenn wir mit diesen Daten nicht viel anfangen können, so werden sie doch meistens automatisch Teil der Datei und damit Gegenstand der Verarbeitung. Damit wir diese Daten bei unserer Verarbeitungstätigkeit und auch bei allen weiteren Verarbeitungstätigkeiten nicht mehr berücksichtigen müssen, lagern wir sie später wieder in eine eigene Verarbeitungstätigkeit aus.

Bei diesen „übergreifenden“ Verarbeitungstätigkeiten ist es häufig nicht möglich und auch nicht sinnvoll, einen Ablauf zu dokumentieren. In den meisten Fällen können Sie den Umgang mit diesen Daten direkt im Ablauf der jeweiligen Verarbeitungstätigkeit dokumentieren. Wenn Sie jedoch feststellen, dass sich Abläufe wiederholen, kann es sinnvoll sein, auch eine Richtlinie für eine „übergreifende“ Verarbeitungstätigkeit zu erstellen.

Sie sehen: Ein Verarbeitungsverzeichnis mit vielen Verarbeitungstätigkeiten bedeutet nicht automatisch mehr Aufwand. Im Gegenteil, diese Vorgehensweise kann Ihnen Zeit ersparen und die Transparenz gegenüber Ihren betroffenen Personen erhöhen. Gerade in der Anfangsphase werden Sie bei der Erstellung einer Verarbeitungstätigkeit immer wieder neue Verarbeitungstätigkeiten entdecken, sodass Ihre – ohnehin schon prall gefüllte – To-do-Liste mit fortschreitender Umsetzung immer länger wird. Aber lassen Sie sich

nicht entmutigen – schon bald werden Sie einen Punkt erreichen, ab dem Ihre To-do-Liste zusehends kürzer wird. Bleiben Sie dran!

Zurück zu unserer Verarbeitungstätigkeit: Daten in Auftragsbestätigungen oder Rechnungen sowie E-Mails mit „Standarddaten“ müssen wir jetzt nicht mehr bei der Ermittlung der personenbezogenen Daten berücksichtigen. Als Datenart benötigen wir sie aber später noch für unser Löschkonzept. Werfen wir nun einen Blick auf die Daten, die für die Erstellung und Verwaltung von Visitenkarten noch von Bedeutung sind:

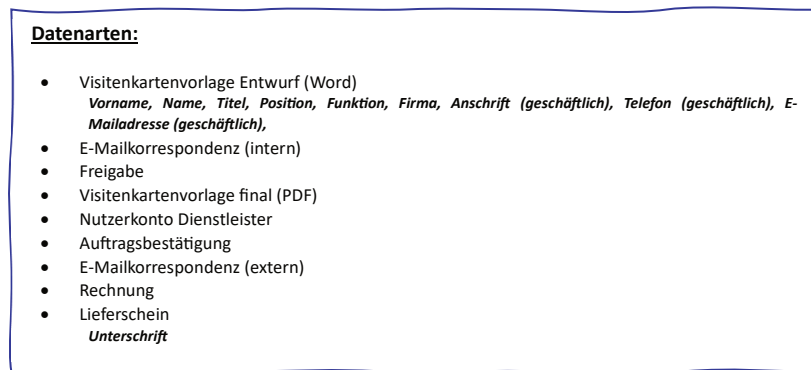


Abbildung 7: Datenarten mit personenbezogenen Daten (angepasst)

Puh, das sieht ja schon viel besser aus! Wir wissen jetzt also, welche Daten wir verarbeiten, wenn wir Visitenkarten erstellen und verwalten wollen. Daten, die wir bereits bei einer Datenart erfasst haben und die sich wiederholen, brauchen nicht nochmals aufgelistet werden. Durch das systematische Durchgehen der verschiedenen Datenarten konnten wir auf einfache Weise eine Übersicht über die personenbezogenen Daten erstellen und so die Gefahr, etwas zu vergessen, verringern.

Jetzt müssen wir noch die Daten zu Kategorien für unser Verzeichnisse zusammenfassen, und schon sind wir auch hier fertig:

Ende der Leseprobe