Checkliste

INFORMATIONSPFLICHTEN

An alles gedacht?

Hinweise zur Anwendung

Diese CHECKLISTE dient der Orientierung und Veranschaulichung zur Umsetzung von Informationspflichten aus der DSGVO. Die Inhalte der Informationspflichten sind gesetzlich in den Artikeln 13 und 14 der DSGVO vorgegeben.

In einer Checkliste haben wir alle Punkte zusammengestellt, welche zu berücksichtigen wären, wenn Sie Ihre Datenschutzhinweise erstellen und diese kurz erläutert. Sie brauchen die Angaben nur machen, wenn diese auch auf Sie zutreffen.

? **FRAGE EINES FREUNDES:** „Warum kann ich nicht einfach den Generator für Datenschutzhinweise nutzen?“

! **ANTWORT:** „Datenschutzhinweise sollten die Gegebenheiten/Verarbeitungen Ihres Unternehmens widerspiegeln. Unser Generator für Datenschutzhinweise deckt grundsätzliche Themen ab, kann aber nicht alles individuell berücksichtigen. Mit dieser Checkliste sind Sie in der Lage jede Informationspflicht für eine Verarbeitung umsetzen.“

Zeigen Sie doch einfach, was Sie tun!

- Die Informationen müssen präzise, transparent, verständlich sein (also nicht zu langatmig).
- Sie sollen nur bereitgestellt werden und dabei leicht zugänglich sein (langes Suchen vermeiden, leichtes Auffinden ermöglichen).
- Die Sprache darf dabei klar und einfach sein – besonders bei Angeboten, welche sich an Kinder richten.
- Die Information ist zum Zeitpunkt der Erhebung bereitzustellen. Es genügt ein deutlicher Hinweis auf die Datenschutzhinweise. Zum Beispiel wird auf der Webseite auf diese verlinkt, im Ladengeschäft werden diese ausgehangen und bei einem schriftlichem Vertragsabschluss, diese am besten als Anlage beigefügt.
- Die Datenschutzhinweise müssen nicht schriftlich gegengezeichnet werden. Das Bestätigen oder Akzeptieren von oder Einwilligen in Datenschutzhinweise sollte unterbleiben.
- Datenschutzhinweise sind eine reine Pflicht der Informationsbereitstellung. Sie sind nicht in Stein gemeißelt und können jederzeit ergänzt und korrigiert werden.
- Informieren Sie lieber zunächst allgemein als gar nicht und verfeinern Sie nach und nach.
- Beugen Sie durch gute Datenschutzhinweise Missverständnissen und Nachfragen von betroffenen Personen vor.

Datenschutzhinweise bereitstellen

Für jede Verarbeitung von personenbezogenen Daten müssen Informationen zur Datenverarbeitung bereitgestellt werden. Folgende Informationen müssen die Datenschutzhinweise enthalten:

- ☐ Die Überschrift
- ☐ Verantwortlicher und sein Vertreter
- ☐ Mit dem Datenschutz beauftragte Person (bei Benennungspflicht Kontaktdaten angeben)
- ☐ Zwecke der Verarbeitung
- ☐ Rechtsgrundlage der Verarbeitung
- ☐ Empfänger von Daten
- ☐ Empfänger in einem Drittland (z.B. USA)
- ☐ Speicherdauer, Löschen
- ☐ Betroffenenrechte
- ☐ Widerrufsrecht bei Einwilligung
- ☐ Beschwerderecht bei einer Aufsichtsbehörde
- ☐ Vertragliche oder gesetzliche Verpflichtung zur Datenerhebung
- ☐ Automatisierte Entscheidungsfindung, Profiling
- ☐ Datenherkunft

Erläuterung zu den einzelnen Punkten

Überschrift

„Datenschutzhinweise für [*Zwecke oder Personenkreise*]“

TIPP: Vergeben Sie eine Überschrift, die zum Inhalt der jeweiligen Datenschutzhinweise passt und nennen Sie nicht alle Dokumente „Informationspflichten nach Art.13 DSGVO“

Verantwortlicher und sein Vertreter

...oder auch: „An wen kann ich mich wenden?“

Verantwortlicher: Wenn Sie über die Zwecke und Mittel einer Verarbeitung entscheiden, dann sind Sie für die Verarbeitung verantwortlich im Sinne der DSGVO. In dem Fall müssen Sie hier Ihre genaue Firmierung und die Kontaktdaten angeben.

- ✓ Bei natürlichen Person: Vor- und Nachname
- ✓ Personengesellschaften und juristischen Personen: Firmenname samt Rechtsformzusatz, z.B. ABC GbR, XYZ GmbH, 0815 OHG, 007 AG
- ✓ Zzgl. Adresse und Kontaktdaten

Vertreter: Mit Vertreter gem. DSGVO ist nicht der Geschäftsführer gemeint, sondern der benannte Firmenvertreter in der EU von nicht in der EU ansässigen Firmen. Sofern Sie als solcher tätig sind, müssen Sie hier die Firmen- und Kontaktdaten angeben. Sonst lassen sie diese Angabe weg.

Mit dem Datenschutz beauftragte Person (bei Benennungspflicht Kontaktdaten angeben)

ALTERNATIVE A) Wenn Sie keinen Datenschutzbeauftragten benannt haben, können Sie Punkt 3 einfach weglassen. Jede Person kann sich auch an den Verantwortlichen unter Nummer 1 direkt wenden.

ALTERNATIVE B) Auch ohne Benennung können Sie eine Person angeben, welche als Ansprechperson für den Datenschutz kommuniziert werden soll.

ALTERNATIVE C) Wenn Sie formell einen Datenschutzbeauftragten ernannt und bei der Aufsichtsbehörde gemeldet haben, dann tragen Sie hier mindestens seine Kontaktdaten ein und stellen Sie die Erreichbarkeit des Datenschutzbeauftragten sicher.

- Zum Beispiel: datenschutz@firma.de
- (ggf. weitere Kontaktmöglichkeiten)
- (Der Name des Datenschutzbeauftragten kann, muss nicht angegeben werden.)

Zwecke der Verarbeitung

Hier informieren Sie mit einfachen Worten über die Zwecke Ihrer Datenverarbeitung. Eine Datenverarbeitung sollte **weder überraschend, noch versteckt erfolgen.**

Zwecke der Verarbeitung können z.B. ein Vertragsabschluss, die Webseitennutzung, der Newsletter-Versand, die allgemeine Kommunikation, ein Gewinnspiel, eine Aufnahme in eine Vertriebsdatenbank, die Vorhaltung einer Kundenhistorie über die Gewährleistungsfrist hinaus oder die Durchführung eines Arbeitsverhältnisses sein. Die Variablen sind mannigfaltig.

Rechtsgrundlage der Verarbeitung

Grundsatz: Keine Datenverarbeitung ohne eine Rechtsgrundlage gemäß Artikel 6 DSGVO! Die Rechtsgrundlage steht im engen Zusammenhang mit dem jeweiligen Zweck. Gängige Rechtsgrundlagen zu den jeweiligen Zwecken sind:

- Art. 6 Abs. 1 a DSGVO
  Die Einwilligung als Rechtsgrundlage für den Versand eines Newsletters.
- Art. 6 Abs. 1 b DSGVO
  Ein Vertragsverhältnis als Rechtgrundlage für die Datenverarbeitung bei der Vertragsdurchführung oder Vertragsanbahnung.
- Art. 6 Abs. 1 c DSGVO
  Eine gesetzliche Vorgabe aus dem Steuerrecht als Rechtsgrundlage zur Aufbewahrung von personenbezogenen Daten.
- Art. 6 Abs. 1 d DSGVO
  Der Schutz eines lebenswichtigen Interesses – z.B. ein medizinischer Notfall – als Rechtsgrundlage.
- Art. 6 Abs 1 e DSGVO
  Aufgaben des öffentlichen Interesses oder die Ausübung öffentlicher Gewalt als Rechtsgrundlage der Verarbeitung.
- Art. 6 Abs 1 f DSGVO
  Das legitime berechtigte Interesse des Verantwortlichen als Rechtsgrundlage einer Datenverarbeitung. Bei einem berechtigten Interesse ist dieses entsprechend anzugeben.

Hinweis zu Art. 6 Abs. 1 f DSGVO – Berechtigtes Interesse

Ein **berechtigtes Interesse** nach Art. 6 Abs. 1 f DSGVO dürfen Sie immer dann als Rechtsgrundlage angeben, wenn die Interessen legitim sind und die Interessen einer betroffenen Person NICHT überwiegen. Hierzu ist eine Interessenabwägung durchzuführen, die intern zu dokumentieren ist.

Das berechtigte Interesse steht im direkten Zusammenhang mit Art. 6 Abs.1 f DSGVO und sollte konkret angegeben werden. Bei Verarbeitungen mit starken Eingriff in die Persönlichkeitsrechte ist eine umfassende Interessenabwägung durchzuführen. Das berechtigte Interesse ist konkret in den Datenschutzhinweisen zu bezeichnen.

Empfänger von Daten

Wenn Sie die personenbezogenen Daten weiterleiten, informieren Sie die Personen darüber und benennen Sie die konkreten Empfänger zumindest jedoch die Kategorien von Datenempfängern. Wie bei der Benennung der Zwecke sollte eine Datenweitergabe **weder überraschend noch versteckt** erfolgen.

Empfänger in einem Drittland (z.B. USA)

Auch eine Datenübermittlung in ein anderes Land (außerhalb der EU und des Europäischen Wirtschaftsraums) ohne gleichwertigen Datenschutzniveau ist der betroffenen Person anzugeben. Ein Drittland gemäß der DSGVO sind Länder, welche kein angemessenes Datenschutzniveau haben.

Sollen Datenübermittlungen in ein Drittland ohne einem Angemessenheitsbeschluss der Kommission durchgeführt werden, müssen geeignete oder angemessene Garantien nachgewiesen werden.

Besondere häufige Relevanz hat das Thema Drittlandtransfer bei der Gestaltung von Webseiten und bei der Nutzung von Cloud-Diensten und/oder webbasierten Softwareanbietern, wo oftmals US-Dienstleister zum Einsatz kommen und zwar direkt oder als Subdienstleister.

Speicherdauer, Löschen

FAUSTREGEL: Wenn Sie personenbezogene Daten für einen bestimmten Zweck erheben und verarbeiten, müssen Sie diese auch wieder löschen, wenn der Zweck für die Verarbeitung entfallen ist.

Die betroffene Person soll darüber informiert werden, wie lange Sie die Daten speichern werden. Wenn es Ihnen nicht möglich ist, einen genauen Zeitpunkt oder eine genaue Zeitspanne zu nennen, dann geben Sie zumindest die Kriterien – also Ihre Entscheidungsmerkmale – an, nach denen Sie die Daten speichern.

Zum Beispiel können Sie buchungsrelevante Dokumente oder Geschäftsfälle nicht einfach umgehend löschen, wenn ein Vertragszweck erfüllt ist, weil Sie nach dem Steuerrecht eine gesetzliche Pflicht zur Aufbewahrung haben.
Wenn Sie die Daten z.B. nach einer Vertragserfüllung nicht löschen, weil Sie diese noch für andere legitime Zwecke benötigen, so sollten Sie auch darüber informieren.

Beispieltext zur Speicherdauer

Speicherdauer
Wir speichern personenbezogene Daten

- solange es zur Erfüllung eines mit Ihnen bestehenden Vertragsverhältnisses oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Rechtsgrundlage: Art. 6 Abs. 1 S. 1 b DSGVO),
- sowie bis zum Ablauf der steuer- und handelsrechtlichen Aufbewahrungsfristen (Rechtsgrundlage: Art. 6 Abs. 1 S. 1 c DSGVO).
-

Die Fristen nach Handelsgesetzbuch und Abgabenordnung zur Aufbewahrung bzw. Dokumentation betragen zwischen 6 bis zehn Jahre.

Nach Fristablauf löschen wir die Daten, es sei denn, dass Sie der Weiterverwendung ausdrücklich eingewilligt haben. (Rechtsgrundlage: Art. 6 Abs. 1 S. 1 a DSGVO).

Im Fall einer einfachen, informatorischen Kontaktanfrage ohne Vertragsbezug erfolgt die Löschung der gespeicherten personenbezogenen Daten, soweit wir davon ausgehen können, dass sich der Grund Ihrer Anfrage erledigt hat und keine entgegenstehenden gesetzliche Aufbewahrungsfristen, die wir zu beachten haben, bestehen.

Über darüberhinausgehende andere Speicherfristen informieren wir Sie in den entsprechenden Abschnitten unserer Datenschutzhinweise.

Betroffenenrechte

Die Umsetzung von Betroffenenrechten hat einen großen Stellenwert in der DSGVO. Betroffene Personen sollen jederzeit die Möglichkeit haben ihre Rechte in Anspruch nehmen zu können. Es ist ausreichend, wenn Sie in Ihren Datenschutzhinweisen allgemein über die Rechte und über die Kontaktmöglichkeiten informieren.

Beispieltext für den Hinweis auf Betroffenenrechte

Sie haben das Recht darauf

Auskunft darüber zu erhalten, ob und welche Daten wir über Sie gespeichert haben (Art. 15 DSGVO),

eine Einwilligung (sofern erteilt) für die Zukunft zu **widerrufen** (Art. 7 Abs. 3 DSGVO),

der Verarbeitung Ihrer Daten zu **widersprechen**, soweit die Verarbeitung auf unser

berechtigtes Interesse beruht und dafür Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben (Art. 21 DSGVO),

dass unrichtige Daten über Sie bei uns **berichtigt** werden (Art. 16 DSGVO),

die unverzügliche **Löschung** Ihrer personenbezogenen Daten zu verlangen (Art. 17 DSGVO),

dass unter bestimmten Bedingungen die Verarbeitung Ihrer Daten **eingeschränkt** wird (Art. 18 DSGVO) und

auf **Datenübertragbarkeit,** wonach wir Ihre Daten an Dritte übertragen oder Ihre Daten in einem maschinenlesbaren Format zu erhalten (Art. 20 DSGVO)

auf **Beschwerde** bei einer Aufsichtsbehörde (Art. 77 DSGVO)

Widerrufsrecht bei Einwilligung

Das Widerrufsrecht gehört zu den Betroffenenrechten und ist als solches wie die anderen Rechte zu erwähnen. Da es im direkten Zusammenhang mit einer Einwilligung steht, ist auf das Widerrufsrecht beim Einholen der Einwilligung hinzuweisen.
Eine korrekte *Formulierung im Rahmen einer Einwilligung wäre z.B.:*

Beispieltext zum Widerrufsrecht

Sie können Ihre gegebene Einwilligung jederzeit widerrufen. Hierzu genügt eine einfache Nachricht an uns. Durch den Widerruf Ihrer Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Beschwerderecht bei einer Aufsichtsbehörde

Jeder betroffenen Person soll es möglichst einfach gemacht werden seine Rechte anwenden zu können. Jede betroffene Person kann sich daher auch direkt an eine Aufsichtsbehörde wenden. Hierüber müssen Sie informieren. Stellen Sie unabhängig davon sicher, dass Sie erreichbar sind und auf Anfragen zum Datenschutz zeitnah reagieren können.

Beispieltext
Wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei einer Aufsichtsbehörde beschweren.

Vertragliche oder gesetzliche Verpflichtung zur Datenerhebung

Benötigen Sie bestimmte Daten, um einen Vertrag überhaupt abschließen zu können, dann ist die Vertragsperson darüber zu informieren, DASS Sie die Daten zur Vertragsdurchführung benötigen und diese verpflichtend anzugeben sind. Eine Freiwilligkeit ist damit nicht mehr gegeben und es kommt hierfür auch keine Einwilligung in Betracht. Notwendige Daten für einen Vertragsabschluss sind daher von anderen Datenverarbeitungen zu unterscheiden.
Sofern der Vertragspartner keine Daten angeben möchte, müssen Sie über die Konsequenzen informieren, d.h. welche Folgen die Nichtbereitstellung hat. Dasselbe trifft auf eine Datenerhebung aufgrund einer gesetzlichen Verpflichtung zu.

Beispieltext für Vertragsabschluss

Die Bereitstellung Ihrer personenbezogenen Daten ist für den Abschluss und Durchführung des Vertrages mit Ihnen im Rahmen der vorvertraglichen Maßnahmen erforderlich. Zur Erhebung der erforderlichen Daten sind wir nach steuerlichen Vorschriften verpflichtet. Stellen Sie uns diese Daten nicht zur Verfügung, ist ein entsprechender Vertragsabschluss oder die Durchführung der vorvertraglichen Maßnahmen nicht möglich

Automatisierte Entscheidungsfindung, Profiling

Entfaltet eine Bewertung einer betroffenen Person rechtliche Wirkung ihr gegenüber oder beeinträchtigt eine Bewertung die betroffenen Person erheblich UND beruht diese Bewertung und Entscheidung ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling –sind Informationen über die eingesetzte Logik des Profiling und der automatisierten Entscheidungsfindung und auch die Auswirkung auf den Betroffenen darzustellen.

Es sollte für den Betroffenen klar werden, woher die verwendeten Daten stammen und welchen Einfluss diese im Rahmen der automatisierten Bewertung auf die Entscheidung haben. Dies betrifft z.B. Werte aus Bonitätsauskünfte und Scoring, die automatisiert eine Entscheidung über die Zahlungsmittel oder des Vertragsabschlusses an sich begründen.

Datenherkunft

Wenn Sie die Daten nicht von der betroffenen Person erhalten, sondern von Dritten, wie z. B. vom früheren Arbeitgeber, der Bank, der Schufa, einem Adresshändler. Oder öffentlichen Quellen, wie Zeitung, Internet, Rundfunk, Flyern, Branchen- oder Telefonverzeichnissen, Registern beziehen, dann müssen Sie auch hierüber informieren.

Tipp: Im Fall einer automatisierten Erhebung, die den Betroffenen nicht unbedingt bewusst ist, sollten Sie über die Datenerhebung informieren. Dies betrifft beispielsweise die automatische Verarbeitung von Browserdaten (IP-Adressen, Browser-Einstellungen etc.) bei Aufruf der Webseite.

Beispieltext für SERVER-LOG-FILES

Bei Nutzung der Webseite werden an den Server, auf welchem sich diese Webseite befindet, über Ihren Browser folgende Informationen automatisch übermittelt (soweit Ihr Browser diese bereitstellt) und in so genannten „Server-Logfiles“ temporär gespeichert:

IP-Adresse (ggf.: in anonymisierter Form),
Datum und Uhrzeit der Anforderung,
Namen der angeforderten Datei,
Dateinamen, von der aus die Datei angefordert wurde,
übertragene Datenmenge,
Zugriffsstatus,
Beschreibung des verwendeten Webbrowsers und Betriebssystems
Namen des Internet Service Providers des Besuchers

Die Erhebung und Verarbeitung erfolgt auf Grund unserer berechtigten Interessen (Art.6 Abs.1 f DSGVO), um die Nutzung der Webseite zu ermöglichen, sowie zur Gewährleistung der Funktionalität und Stabilität und Sicherheit der Webseite. Die Daten werden nach 7 Tagen gelöscht.