Up to Data:

Leitfaden zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 DSGVO

Pflicht zur Erstellung

Grundsätzlich fordert Art. 30 DSGVO, dass alle Verantwortlichen[1] ein Verzeichnis über die im Unternehmen vorkommenden Verarbeitungstätigkeiten (im Folgenden: VVZ) zu führen haben. Es muss also dokumentiert werden, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird (z.B. Programme zur Kundenverwaltung). Für bestimmte Unternehmen sieht das Gesetz eine Freistellung von der Verpflichtung zu Erstellung vor; nämlich dann, wenn das Unternehmen oder die Einrichtung weniger als 250 Mitarbeiter beschäftigt, wenn die Datenverarbeitung nur gelegentlich erfolgt und wenn keine besonderen Datenkategorien wie Gesundheits- oder Religionsdaten verarbeitet werden. Dadurch, dass beide Voraussetzungen kumulativ vorliegen müssen und die Datenverarbeitung in der Regel nirgends nur gelegentlich erfolgt, hat diese Freistellung in der Praxis kaum Bedeutung. Allerdings galt die Verpflichtung ein solches Verzeichnis zu führen schon vor Inkrafttreten der DSGVO. Es ist also das Herzstück des Datenschutzes in Ihrem Unternehmen. Wir empfehlen daher, den Fokus auf die Erstellung und Pflege des Verzeichnisses zu legen, da sich die Behörde im Falle einer Prüfung dieses vorlegen lassen wird.

Form und Inhalt

Grundsätzlich ist für das VVZ keine bestimmte Form vorgeschrieben. Sie können daher schriftlich oder elektronisch vorgehalten werden. Die Verzeichnisse sind regelmäßig in deutscher Sprache zu führen. Ob eine Excel-Liste oder ein anderes gängiges Muster verwendet wird, ist jedem Verantwortlichen selbst überlassen. Wichtig ist hier nur, dass die Verzeichnisse immer aktuell gehalten werden. Sinnvoll ist es, einmal im Jahr die Verzeichnisse zu überprüfen und etwaige Aktualisierungen / Überschreibungen ebenfalls ein Jahr vorzuhalten.

Art. 30 DSGVO zählt bestimmte Mindestanforderungen an das VVZ:

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener personenbezogener Daten
- Kategorien von Empfängern von Daten / Empfänger in Drittstaaten
- Löschfristen

[1] Verantwortlicher ist jeder, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Beachten Sie hier, dass die Angaben aussagekräftig und für Außenstehende nachvollziehbar sein müssen. Je detaillierter Ihre Angaben hier sind, desto eher kann sich ein Prüfer der Aufsichtsbehörde in diesen Prozess hineindenken.

Vorgehensweise zur Erstellung

1. Einteilung des Unternehmens
   Unterteilen Sie Ihr Unternehmen in organisatorische Bereiche, Einheiten, Abteilungen o.Ä. Diese Einteilung bietet eine Hilfe zur Strukturierung Ihrer Prozesse und hilft Ihnen zudem, die Prozesse herauszuarbeiten. In fast allen Unternehmen werden sich ähnliche Bereiche herauskristallisieren, die mit personenbezogenen Daten arbeiten. Hier reicht es zunächst aus, „Oberbegriffe" herauszuarbeiten.
   - Buchhaltung
   - Personal
   - Marketing
   - …

2. Verarbeitungsprozesse identifizieren
   In einem zweiten Schritt schauen Sie sich die Oberbegriffe an, die Sie für Ihr Unternehmen herausgearbeitet haben und identifizieren in den jeweiligen Bereichen die Verarbeitungstätigkeiten. Gehen Sie hierbei so kleinschrittig wie möglich vor, weil sich manchmal unterschiedliche Löschfristen ergeben.
   Hierzu ein Beispiel:

   Bei Ihnen gibt es wahrscheinlich eine Personalabteilung oder zumindest einen Personalverantwortlichen. In diesem Bereich werden klassischerweise Daten von Mitarbeitern und auch von Bewerbern verarbeitet. Dazu zählen Name, Adresse und Bankverbindung, ggfs. eine Zeiterfassung aber auch sensible Daten wie die Konfession oder Gesundheitsdaten in Form von Krankmeldungen. Diese Daten werden für die allgemeine Personalverwaltung, die Erstellung des Arbeitsvertrags und die Überweisung der Gehälter gebraucht. Bei Bewerbern werden außerdem noch Informationen aus dem Lebenslauf gespeichert. Damit haben Sie Ihre ersten vier Verarbeitungstätigkeiten gefunden: die klassische Personalverwaltung, die Lohn- und Gehaltsabrechnung, die Arbeitszeiterfassung und die Bewerbungen.

3. Verarbeitungsprozesse im Verzeichnis darstellen
   Damit Sie sich die Darstellung der Verarbeitungsprozesse besser vorstellen können, haben wir unten ein Muster-VZZ eingefügt. Zuerst benennen Sie die Verarbeitungstätigkeit und versehen Sie mit einer laufenden Nummer. Dann tragen Sie die Fachabteilung oder den Ansprechpartner für diesen Bereich ein. Als nächstes kreuzen Sie an, um welche betroffenen Personen es sich bei diesem Vorgang handelt oder ergänzen diese Aufzählung entsprechend. Danach müssen Sie die Art der erhobenen Daten aufzählen. Hier muss darauf geachtet werden, dass die besonderen Kategorien (z.B.

Religionszugehörigkeit oder Gesundheitsdaten) extra aufgezählt werden und eine Differenzierung zu den „normalen“ personenbezogenen Daten stattfindet. Als nächstes müssen die Kategorien sämtlicher Empfänger (intern und extern) aufgelistet werden und es muss deutlich gemacht werden, ob auch eine Drittland-Übermittlung erfolgt. Zuletzt müssen Löschfristen ermittelt und benannt werden. Abschließend wäre jeder Vorgang vom Verantwortlichen zu unterschreiben.

Verarbeitungstätigkeit: Benennung: _____		**lfd. Nr.:** _____
Datum der Einführung:	Datum der letzten Änderung:	
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)		
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)		
Optional: Name des eingesetzten Verfahrens		
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐	

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Gern können Sie sich bei Fragen zu diesen Themenkomplexen an uns wenden!

Ihr Team der RKM Data GmbH