Kurzbeschreibung zur Erstellung   
eines Datenverarbeitungsverzeichnisses

Wichtige Hinweise

Diese Wegleitung dient als Hilfe zur Erstellung des *Verzeichnisses von Verarbeitungstätigkeiten* von personenbezogenen Daten im Zuständigkeitsbereich eines Verantwortlichen oder eines Auftragsverarbeiters.

Diese Wegleitung und die Vorlagen stellen eine unverbindliche Information und abstrakte Leitlinien dar, welche sich vor allem an kleinere und mittlere Unternehmen richten. Es kann keine Gewähr für sachliche Richtigkeit, Vollständigkeit und/oder Aktualität im konkreten Anwendungsfall geleistet werden. Bei der praktischen Umsetzung ist jeweils auf die konkreten Anwendungsfälle im Unternehmen abzustellen. Teilweise befinden sich Weisungen der Behörden zum Zeitpunkt der Veröffentlichung dieses Dokuments noch in Vorbereitung. Aufgrund der derzeitigen Entwicklungen im Datenschutzrecht mit unterschiedlichen Anforderungen, Begriffsdefinitionen und Anwendungen sowohl in der EU, den Mitgliedstaaten der EU/EWR (Liechtenstein, Island, Norwegen) wie auch in der Schweiz sowie eines möglichen internationalen Bezugs der Verarbeitungstätigkeit ist eine Zusammenarbeit mit einer Rechtsanwältin/einem Rechtsanwalt Ihres Vertrauens für die massgeschneiderte Ausarbeitung und Prüfung des Verzeichnisses geboten.

1. Was ist ein Verzeichnis?

Das Verzeichnis dient einerseits als Fundament für eine strukturierte Datenschutzdokumentation und der Selbstkontrolle des Verantwortlichen und des Auftragsverarbeiters. Andererseits bildet es die Grundlage für den Nachweis der Rechenschaftspflicht zur Einhaltung der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU). Die DSGVO kann unter folgender Website <http://eur-lex.europa.eu/eli/reg/2016/679/oj> abgerufen werden. Der Wortlaut der einschlägigen Bestimmung für die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten in Art. 30 DSGVO findet sich am Ende dieses Dokuments (Anhang I).

Das Verzeichnis der Verarbeitungstätigkeiten muss die in der DSGVO genannten Mindestangaben enthalten. Die Summe aller Verarbeitungstätigkeiten ergibt das Verzeichnis eines Verantwortlichen oder eines Auftragsverarbeiters.

Da die Angaben im Verzeichnis die Quelle für die Beurteilung der Einhaltung der datenschutzrechtlichen Pflichten der DSGVO bildet, können dem Verzeichnis – zur Erleichterung des Nachweises der Einhaltung der DSGVO – nebst den Mindestangaben des Verzeichnisses gemäss Art. 30 DSGVO, weitere optionale Elemente hinzugefügt werden. Beispiele für solche optionalen Angaben zum *Verzeichnis des Verantwortlichen und des Auftragsverarbeiters* finden sich unter Punkt *IV Optionale Angaben*. In der vorliegenden Vorlage wurden bereits ein paar optionale Angaben zu Illustrationszwecken ins Verzeichnis aufgenommen. Diese werden an den betreffenden Stellen jeweils als optional angegeben.

Jeder Verantwortliche und Auftragsverarbeiter hat die Pflicht, mit der zuständigen Aufsichtsbehörde zusammenzuarbeiten. Daher müssen die Verzeichnisse der Aufsichtsbehörde auf Anfrage zwecks Kontrolle zur Verfügung gestellt werden. Die Verzeichnisse sind schriftlich zu führen. Dies kann auch in einem elektronischen Format erfolgen (Art. 30 Abs. 3 DSGVO).

Die Verzeichnisse müssen stets auf dem aktuellsten Stand sein. Änderungen bei der Datenverarbeitung müssen im Verzeichnis umgehend angepasst werden. Die Anpassungen und deren Datierung sind zu dokumentieren.

2. Wer muss ein Verzeichnis führen?

Grundsätzlich muss jeder, der Personendaten verarbeitet und der DSGVO untersteht, ein Verzeichnis der Datenverarbeitungen führen. Aufgrund der extraterritorialen Wirkung der DSGVO findet diese auch auf viele Datenverarbeiter in der Schweiz Anwendung. Dies ist der Fall, wenn

1. die Datenbearbeitung im Rahmen der Tätigkeiten einer **Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters in der EU erfolgt (unabhängig davon, ob die Verarbeitung in der EU stattfindet (Art. 3 Abs. 1 DSGVO), oder
2. **ohne Niederlassung** in der EU (Art. 3 Abs. 2 DSGVO), wenn die Datenverarbeitung im Zusammenhang damit steht:
   1. betroffenen Personen in der EU *Waren oder Dienstleistungen anzubieten* (unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist), oder
   2. das *Verhalten betroffener Personen zu beobachten,* soweit ihr Verhalten in der EU erfolgt (Art. 3 Abs. 2 DSGVO).

Eine Ausnahme von der Führung eines Verzeichnisses gilt lediglich für Unternehmen oder Einrichtungen, die **weniger als 250 Mitarbeiter** beschäftigen und sofern die von ihnen vorgenommene Verarbeitung:

* + kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
  + nur gelegentlich erfolgt oder
  + keine Verarbeitung besonderer Datenkategorien bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche *Verurteilungen und Straftaten* einschliesst.

Unter Berücksichtigung, dass Datenverarbeitungen typischerweise regelmässig erfolgen und die Verarbeitungen auch selten ohne Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden sind, ist davon auszugehen, dass diese Ausnahmen nur selten greifen. Da das Verzeichnis auch die Grundlage für die Beurteilung der Rechtmässigkeit der Datenverarbeitungen bildet, ist es sinnvoll und empfehlenswert, ein solches Verzeichnis zu führen, selbst wenn keine Pflicht dazu besteht.

Die Schweizer Unternehmen, die der DSGVO unterstehen (vgl. oben), müssen zudem schriftlich einen **Vertreter** in der Europäischen Union benennen und diesen im Verzeichnis angeben (EU-Vertreter) (Art. 27 Abs. 1 DSGVO). Der Vertreter hat insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der Verordnung als Anlaufstelle zu dienen.

Die Pflicht zur Benennung eines EU-Vertreters entfällt nur in den folgenden Fällen:

* + wenn eine Verarbeitung nur gelegentlich erfolgt,
  + nicht umfangreiche besondere Datenkategorien im Sinne von Art. 9 Abs. 1 DSGVO oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO einschliesst,
  + unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, sowie
  + für Behörden oder öffentliche Stellen.

Analog der oben aufgeführten Ausnahme von der Führung eines Verzeichnisses und der tief angesetzten Schwellen ist auch bei der Bestellung des EU-Vertreters davon auszugehen, dass die Ausnahme nur selten greift.

Die vorliegende Wegleitung enthält Erläuterungen und Beispiele (in Blau ausgewiesen) als Orientierungshilfe, welche direkt im Formular aufgeführt sind. Die Erläuterungen sowie die Beispiele sind jeweils bei der Erfassung der konkreten Verarbeitungstätigkeit zu löschen.

Begriffsdefinitionen gemäss DSGVO

|  |  |
| --- | --- |
| Personenbezogenen Daten: | Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen (Art. 4 Abs. 1 DSGVO). |
| Besondere Kategorien personenbezogener Daten: | Besondere Kategorien personenbezogener Daten sind: Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DSGVO). |
| Verantwortlicher:  Gemeinsam Verantwortliche: | Verantwortlicher ist die 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 (Englisch: Controller [C]) (Art. 4 Abs. 7 DSGVO).  Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art. 26 DSGVO). |
| Auftragsverarbeiter: | Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Englisch: Processor [P]) (Art. 4 Abs. 8 DSGVO). |
| EU-Vertreter: | Eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäss Art. 27 DSGVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach der DSGVO obliegenden Pflichten vertritt (Art. 4 Abs. 17 DSGVO). |

|  |  |
| --- | --- |
| 1. Allgemeine Angaben und Kontaktinformationen | *Erläuterungen:*  *Die Angaben in Ziffer 1.2 –1.6 dienen der Identifizierung des Verantwortlichen und gegebenenfalls weiterer zuständiger und involvierter Personen.* |
| 1.1 Name und Kontaktangaben des Verantwortlichen (Firma/Name der juristischen Person)  (Name, Adresse, Telefon, E-Mail, Internetadresse) |  |
| 1.2 gesetzliche Vertretung  (Name, Adresse, Telefon, E-Mail der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.3 gegebenenfalls Name und Kontaktangaben eines gemeinsam Verantwortlichen (Co-Controller)  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.4 gegebenenfalls Name und Kontaktangaben des EU-Vertreters des Verantwortlichen  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.5 Name und Kontaktangaben eines etwaigen Datenschutzbeauftragten  (Name, Adresse, Telefon, E-Mail, Internetadresse) |  |
| 1.6 optional: gegebenenfalls Name und Kontaktangaben von weiteren Unternehmensabteilungen, die Auskunft über die Datenverarbeitung geben können |  |

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gemäss Art. 30 Abs. 1 DSGVO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Angaben zur Verarbeitungstätigkeit | | | | |
| Interne Nummer: | Datum der Einführung: | | Datum der letzten Änderung: | *Erläuterungen:* |
| 2.1 Bezeichnung der Verarbeitungstätigkeit | | Beispiele:  allgemeine Kundenverwaltung  Online-Marketing  Bewerber-Management | | *An dieser Stelle ist die Bezeichnung der dokumentierten Verarbeitungstätigkeit anzugeben. Es ist zu empfehlen, eine im Unternehmen gebräuchliche Bezeichnung des Geschäftsprozesses zu wählen.*  *Eine Verarbeitungstätigkeit bzw. ein Geschäftsprozess kann aus mehreren Teilprozessen bestehen, die unterschiedlichen Zwecken dienen können. Um dem Kontrollzweck des Verzeichnisses nachzukommen und zum Zweck der Prüfung der Vereinbarkeit mit der DSGVO, ist zu empfehlen, dass die Verarbeitungstätigkeiten generell zu fein als zu grob gegliedert werden. Dies umso mehr bei Verarbeitungstätigkeiten, die ein erhöhtes Risiko für die betroffenen Personen zur Folge haben können (z.B. Verarbeitung besonderer Kategorien personenbezogener Daten [wie z.B. Gesundheitsdaten, Religion], Profiling, Tracking, Verwendung neuer Technologien, grosse Datenmengen etc.).* |
| 2.2 Zwecke der Verarbeitung | | Beispiele von Zwecken der Verarbeitungstätigkeit gemäss obiger Ziffer 2.1.  „Allgemeine Kundenverwaltung“: Zwecke der Verarbeitung: „Buchhaltung und Inkasso“  „Online-Marketing“; Zwecke der Verarbeitung: „Newsletter, zielgerichtete Werbung, Gewinnspiele“  «Bewerber-Management»: Zwecke der Verarbeitung: Evaluieren von möglichen neuen Arbeitnehmern zum Zweck der Anstellung durch Abschluss eines Arbeitsvertrags | | *Hier anzugeben sind für jede Verarbeitung die Zwecke der Verarbeitung. Als Hilfestellung für die Zweckbestimmung können die Gründe für die Datenerhebung, die Aufgaben oder Ziele der Verarbeitung angegeben werden.*  *Die Zwecke müssen eindeutig und vollständig sein, damit die Angemessenheit der getroffenen Schutzmassnahmen und die Zulässigkeit der Verarbeitung geprüft werden können.* |
| 2.3 Beschreibung der Kategorien betroffener Personen | | Beispiele: Kunden, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. | | *An dieser Stelle sind Kategorien oder Personengruppen, deren persönlichen Daten in der eingangs aufgeführten Verarbeitungstätigkeit für die in Ziffer 2.2 aufgeführten Zwecke bearbeitet werden, anzugeben.* |
| 2.4 Beschreibung der Kategorien personenbezogener Daten | | Beispiele:  Kunden: Name, Vorname, Adressdaten, Telefon, E-Mail, Geburtsdatum, Vertragsdaten, Bonitätsdaten, Produktinteresse, in der Vergangenheit getätigte Geschäfte/Einkäufe, Bankverbindung.  Arbeitnehmer: Name, Vorname, Kontaktdaten, Bankverbindung, Sozialversicherungsdaten etc.  besondere Kategorien personenbezogener Daten  Beschreibung:  personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten  Beschreibung: | | *An dieser Stelle anzugeben sind für jede Verarbeitung die Kategorien personenbezogener Daten, die von den einzelnen Kategorien oder Personengruppen erhoben werden. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen/Datenkategorien" gemeint.*  *Die Bezeichnungen der Datenkategorien müssen so konkret wie möglich sein. Unzureichend sind allgemeine Angaben wie beispielsweise "Mitarbeiterdaten" oder "Kundendaten".* |
| 2.5 Optional: Rechtsgrundlage der Verarbeitungen / Verarbeitungstätigkeit | | Einwilligung der betroffenen Person  für die Erfüllung eines Vertrags mit der betroffenen Person  für die Erfüllung einer rechtlichen Verpflichtung (detaillierte Beschreibung):  erforderlich zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Beschreibung):  weitere Gründe (Beschreibung): | | *Hier anzugeben ist die einschlägige Rechtsgrundlage der Verarbeitungstätigkeit gemäss Art. 6 DSGVO. Beispiele für mögliche Rechtsgrundlagen sind aufgeführt. Es ist jeweils die im konkreten Fall vorliegende Verarbeitungstätigkeit anzugeben.* |

|  |  |  |
| --- | --- | --- |
| 2.6 Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschliesslich Empfänger in Drittländern oder internationalen Organisationen | Empfängerkategorien (in EU und Drittländer; beinhaltet auch erst geplante Offenlegungen/Übermittlungen)  intern (Stellen innerhalb des Verantwortlichen)  Personalabteilung, CRM, Buchhaltung, IT  extern (jeder andere Empfänger, auch im Konzernunternehmen, Auftragsverarbeiter, Dritte und internationale Organisationen)  Konzernunternehmen  als Auftragsverarbeiter:  Firma, Adresse, Land  Personalabteilung, CRM, Buchhaltung, IT  Dokumentation Konzernunternehmen als Auftragsverarbeiter:  Auftragsverarbeiter-Vertrag (Ort der Ablage: Sitz der Unternehmung)  als Dritter (verarbeitet die Daten für eigene Zwecke und ist damit selbst ein Verantwortlicher):  Firma, Adresse, Land  Personalabteilung, CRM, Buchhaltung, IT  Dokumentation Konzernunternehmen  vertragliche Grundlage (Ort der Ablage: Sitz der Unternehmung)  Auftragsverarbeiter  Firma, Adresse, Land  Dokumentation zum Auftragsverarbeiter  Auftragsverarbeiter-Vertrag (Ort der Ablage: Sitz der Unternehmung)  weitere Dritte  Firma, Adresse, Land  Dokumentation zum Dritten  vertragliche Grundlage (Ort der Ablage: Sitz der Unternehmung)  internationale Organisationen:  Name, Adresse, Land  Dokumentationsgrundlagen:  Bezeichnung des Vertrags und Ort der Ablage: Sitz der Organisation | *Kategorien von Empfängern sind weitere Stellen oder Fachabteilungen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten planmässig erhalten sollen. Zu erfassen sind auch Auftragsverarbeiter oder Dritte. Ausgenommen sind lediglich Behörden, die für einen bestimmten Untersuchungsauftrag möglicherweise personenbezogene Daten erhalten (Art. 4 Abs. 9 Satz 2 DS-GVO).*  *Irrrelevant ist, ob es sich um eine aktive Übertragung oder einen Direktzugriff des Empfängers auf die persönlichen Daten handelt.*  *Drittländer sind Länder, welche nicht oder nicht mehr zu den EU-Mitgliedstaaten gehören. Beispiele für internationale Organisationen sind Institutionen der UNO oder der EU.*  *Als optionale Angaben kann für jede externe Empfängergruppe nebst der Bezeichnung der Rechtseinheit die jeweilige Vertragsgrundlage wie z.B. der Auftragsverarbeiter-Vertrag und der Ort der Ablage zu Dokumentationszwecken angegeben werden.* |
| 2.7 Weitere Angaben zu Datenübermittlungen an Drittländer oder an internationale Organisationen (ausserhalb der EU), einschliesslich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie bei den in Art. 49 Abs. 1 Untersatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien | Name des Drittlands oder der internationalen Organisation:  z.B. China, Indien, USA, Liechtenstein  [ggf. Verweis auf vorherigen Punkt 2.6]  Beschreibung geeigneter Garantien zum Schutz der personenbezogenen Daten im jeweiligen Drittland gemäss Art. 49 Abs. 1 Untersatz 2 DSGVO sowie die vorgenommene Beurteilung:  Dokumentation weiterer geeigneter Garantien  anerkannter Drittstaat  EU-Standardvertrag C/C  EU-Standardvertrag C/P  verbindliche interne Datenschutzvorschriften  andere | *Da ein Datentransfer in Drittländer oder an internationale Organisationen ein erhöhtes Gefährdungspotenzial für die Betroffenen begründet, sind entsprechende Angaben im Verzeichnis notwendig.*  *Konkret zu benennen ist insbesondere das betreffende Drittland oder die betreffende internationale Organisation.*  *Ferner zu dokumentieren sind die vom Verantwortlichen vorgenommene Beurteilung sowie die angemessenen Garantien zum Schutz der personenbezogenen Daten im Drittland, sofern eine Übermittlung für bestimmte Fälle gemäss Art. 49 Abs. 1 Untersatz 2 DSGVO erfolgt.*  *Als optionale Angaben können, sofern keine Übermittlung für bestimmte Fälle im Sinne von Art. 49 Abs. 1 Untersatz 2 DSGVO erfolgt (vgl. obiger Absatz), die geeigneten Garantien auf Grundlage eines Angemessenheitsbeschlusses oder anderer geeigneter Garantien wie z.B. die EU-Standarddatenschutzklauseln, verbindlichen internen Datenschutzvorschriften oder andere Garantien gemäss Art. 46 DS-GVO zum Zweck der Dokumentationspflicht angegeben werden. Selbst wenn es sich hierbei um optionale Angaben handelt, ist es empfehlenswert, die Dokumentation weiterer geeigneter Garantien ins Verzeichnis aufzunehmen.* |
| 2.8 Vorgesehene Fristen für die Aufbewahrungsdauer/Löschung der verschiedenen Datenkategorien; falls dies nicht möglich ist, Beschreibung der Kriterien für die Festlegung der Fristen |  | *Anzugeben sind die vorgesehenen Löschfristen der verschiedenen Datenkategorien, falls unterschiedliche Löschfristen bestehen. Allgemeine Angaben genügen nicht, sondern es sind präzise Angaben zu machen.*  *In der Regel richtet sich die Löschung nach dem Zweck der Datenverarbeitung. Eine Löschpflicht besteht grundsätzlich unverzüglich nach Erfüllung des Zwecks. Ausnahmen ergeben sich insbesondere aus gesetzlichen Aufbewahrungspflichten, wie z.B. aus dem Obligationenrecht, Steuerrecht oder sonstigen branchenspezifischen Rechtsvorschriften.* |
| 2.9 Optional: Beschreibung der eingesetzten IT-Infrastruktur für die Datenverarbeitung, wie beispielsweise Anlagen, Software, Systeme, Einrichtungen und Gegebenheiten, Datahosting, Cloud-Dienste, Bezeichnung des Infrastrukturbetreibers und Ort des Datenservers/der Datenspeicherung | Daten auf eigener Hardware gespeichert  Bezeichnung des Systems  Infrastrukturbetreiber  Ort und Land der Datenspeicherung  Daten auf Hardware Dritter gespeichert  Bezeichnung des Systems  Infrastrukturbetreiber  Ort und Land der Datenspeicherung | *Optional können an dieser Stelle Informationen zur genutzten IT-Infrastruktur und Software/Systemlandschaft gemacht werden, welche für die Datenverarbeitung/Datahosting verwendet werden, die Bezeichnung des Infrastrukturbetreibers und zum Ort der Datenspeicherung.* |
| 2.10 Allgemeine Beschreibung der technischen und organisatorischen Massnahmen | Beschreibung der Massnahmen, die beispielsweise folgende Anforderungen erfüllen:  Massnahmen zum Zweck der Sicherstellung der physischen Zugangskontrolle:  Massnahmen zum Zweck der Sicherstellung der elektronischen Zugangskontrolle:  Massnahmen zum Zweck der Sicherstellung der Datenübertragung (Transportkontrolle):  Massnahmen zum Zweck der Sicherstellung der Eingabekontrolle:  Massnahmen zum Zweck der Sicherstellung der Verfügbarkeit der Daten (Datensicherung und Datenwiederherstellung):  Massnahmen zum Zweck der Sicherstellung der getrennten Datenverarbeitung von Daten, die für verschiedene Zwecke erhoben wurden:  Massnahmen zum Zweck der Sicherstellung der Wirksamkeit der technischen und organisatorischen Massnahmen:  Massnahmen zur Pseudonymisierung personenbezogener Daten:  Massnahmen zur Verschlüsselung personenbezogener Daten:  organisatorische Massnahmen zum Schutz personenbezogener Daten: z.B. Implementierung von Datenschutz-Richtlinien, Anweisungen, Schulungen etc.  etc. | *Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Massnahmen zu treffen.*  *Demzufolge ist hier eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen für die Verarbeitungstätigkeit aufzunehmen (Art. 32 DSGVO). Die Beschreibung sollte so umfangreich sein, dass eine Beurteilung darüber gemacht werden kann, ob die getroffenen Massnahmen geeignet sind, die Sicherheit der Verarbeitungen zu gewährleisten.*  *Sofern bereits ein vorhandenes, übergreifendes Sicherheitskonzept besteht, kann auf dieses verwiesen werden. In diesem Fall müssten nur allfällige Abweichungen für die entsprechende Verarbeitungstätigkeit ins Verzeichnis aufgenommen werden.*  *Bei Verweis auf ein entsprechendes separates Sicherheitskonzept-Dokument ist zu beachten, dass dieses gegebenenfalls auch den Behörden vorgelegt werden müsste.* |
| Diese Datenverarbeitung wird in regelmässigen Zeitabständen von [6/9/12] Monaten überprüft. | |  |

Verantwortlicher

……………………………… ……………………………… ………………………………

Datum Name Unterschrift

Verzeichnis von Verarbeitungstätigkeiten   
des Auftragsverarbeiters gemäss Art. 30 Abs. 2 DSGVO

|  |  |
| --- | --- |
| 1. Allgemeine Angaben und Kontaktinformationen | *Erläuterungen:*  *Die Angaben in Ziffer 1.2 – 1. 7 dienen der Identifizierung des Verantwortlichen und gegebenenfalls weiterer zuständiger und involvierter Personen.* |
| 1.1 Name und Kontaktangaben des Auftragsverarbeiters  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.2 Name und Kontaktangaben eines allfälligen weiteren gemeinsamen Auftragsverarbeiters  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.3 gegebenenfalls Name und Kontaktangaben des EU-Vertreters des Auftragsverarbeiters  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gemäss Handelsregister zur Vertretung berechtigten Personen) |  |
| 1.4 Name und Kontaktangaben des Verantwortlichen und allfälliger weiterer Verantwortlicher  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gesetzlichen Vertretung) |  |
| 1.5 gegebenenfalls Name und Kontaktangaben des EU-Vertreters des Verantwortlichen  (Name, Adresse, Telefon, E-Mail, Internetadresse, bei juristischen Personen die Namen der gesetzlichen Vertretung) |  |
| 1.6 Name und Kontaktangaben eines etwaigen Datenschutzbeauftragten  (Name, Adresse, Telefon, E-Mail, Internetadresse) |  |
| 1.7 optional: gegebenenfalls Name und Kontaktangaben von weiteren sachdienlichen Stellen |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Angaben zur Verarbeitungstätigkeit | | | | |
| Interne Nummer: | Datum der Einführung: | | Datum der letzten Änderung: | *Erläuterungen:* |
| 2.1 Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden | | Beispiele:  Hosting, E-Mail-System  Cloud-Services  Finanzbuchhaltung | | *Hier ist die Art der Verarbeitungen mit allfälligen Erläuterungen zu dokumentieren wie z.B. die für den Verantwortlichen zu erbringenden Leistungen. Diese Angaben ergeben sich in der Regel aus dem Auftragsverarbeiter-Vertrag oder diesem zugrunde liegenden Hauptleistungsvertrag.* |
| 2.2 Datenübermittlungen an Drittländer oder an internationale Organisationen (ausserhalb der EU), einschliesslich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie bei den in Art. 49 Abs. 1 Untersatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien | | Name des Drittlands oder der internationalen Organisation:  z.B. China, Indien, USA, Liechtenstein  🞏 Beschreibung geeigneter Garantien zum Schutz der personenbezogenen Daten im Drittland gemäss Art. 49 Abs. 1 Untersatz 2 DSGVO sowie die vorgenommene Beurteilung:  Dokumentation weiterer geeigneter Garantien  anerkannter Drittstaat  EU-Standardvertrag C/C  EU-Standardvertrag C/P  verbindliche interne Datenschutzvorschriften  andere | | *Zu dokumentieren sind die vom Verantwortlichen vorgenommene Beurteilung sowie die angemessenen Garantien zum Schutz der personenbezogenen Daten im Drittland, sofern eine Übermittlung für bestimmte Fälle gemäss Art. 49 Abs. 1 Untersatz 2 DSGVO erfolgt.*  *Als optionale Angaben können, sofern keine Übermittlung für bestimmte Fälle im Sinne von Art. 49 Abs. 1 Untersatz 2 DSGVO erfolgt, die geeigneten Garantien auf Grundlage eines Angemessenheitsbeschlusses oder anderer geeigneter Garantien wie beispielsweise die EU-Standarddatenschutzklauseln, verbindlichen internen Datenschutzvorschriften oder andere Garantien gemäss Art. 46 DS-GVO zum Zweck der Dokumentationspflicht angegeben werden. Selbst wenn es sich hierbei um optionale Angaben handelt, ist es empfehlenswert, die Dokumentation weiterer geeigneter Garantien ins Verzeichnis aufzunehmen.* |
| 2.3 allgemeine Beschreibung der technischen und organisatorischen Massnahmen | | Beschreibung der Massnahmen, die beispielsweise folgenden Anforderungen erfüllen:  Massnahmen zum Zweck der Sicherstellung der physischen Zugangskontrolle:  Massnahmen zum Zweck der Sicherstellung der elektronischen Zugangskontrolle:  Massnahmen zum Zweck der Sicherstellung der Datenübertragung (Transportkontrolle):  Massnahmen zum Zweck der Sicherstellung der Eingabekontrolle:  Massnahmen zum Zweck der Sicherstellung der Verfügbarkeit der Daten (Datensicherung und Datenwiederherstellung):  Massnahmen zum Zweck der Sicherstellung der getrennten Datenverarbeitung von Daten, die für verschiedene Zwecke erhoben wurden:  Massnahmen zum Zweck der Sicherstellung der Wirksamkeit der technischen und organisatorischen Massnahmen:  Massnahmen zur Pseudonymisierung personenbezogener Daten  Massnahmen zur Verschlüsselung personenbezogener Daten:  organisatorische Massnahmen zum Schutz personenbezogener Daten: z.B. Implementierung von Datenschutz-Richtlinien, Anweisungen, Schulungen etc.  etc. | | *Hier aufzuführen ist eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 DSGVO). Die Beschreibung sollte so umfangreich sein, dass eine Beurteilung darüber gemacht werden kann, ob die getroffenen Massnahmen geeignet sind, die Sicherheit der Verarbeitungen zu gewährleisten.*  *Sofern bereits ein vorhandenes, übergreifendes Sicherheitskonzept besteht, kann auf dieses verwiesen werden. In diesem Fall müssten nur allfällige Abweichungen für die entsprechende Verarbeitungstätigkeit ins Verzeichnis aufgenommen werden.*  *Bei Verweis auf ein entsprechendes separates Sicherheitskonzept-Dokument ist zu beachten, dass dieses gegebenenfalls auch den Behörden vorgelegt werden müsste.* |
| Diese Datenverarbeitung wird in regelmässigen Zeitabständen von [6/9/12] Monaten überprüft. | | | |  |

Auftragsverarbeiter

……………………………… ……………………………… ………………………………

Datum Name Unterschrift

Optionale Angaben

Sofern der Verantwortliche oder der Auftragsverarbeiter Ihr Verzeichnis zum Nachweis Ihrer Rechenschafts- und Dokumentationspflichten nutzen möchte, ist es sinnvoll, hierfür zusätzliche Informationen in das Verzeichnis aufzunehmen. Im Verzeichnis des Verantwortlichen können dies beispielsweise folgende Angaben sein:

* die Rechtsgrundlage für die Verarbeitung;
* die Quelle oder die Herkunft der personenbezogenen Daten;
* die Risiken für die betroffenen Personen;
* die eingesetzte IT-Infrastruktur (Hardware/Software) und der Ort des Datenservers (Ort der Datenspeicherung).

In das Verzeichnis des Auftragsverarbeiters können folgende optionale Angaben aufgenommen werden:

* Weisungen des Auftraggebers;
* Genehmigungen des Auftraggebers betreffend Unterauftragsverarbeiter im Sinne von Art. 28 Abs. 2 und 4 DSGVO.

Anhang I

Art. 30 DSGVO

Verzeichnis von Verarbeitungstätigkeiten

1. Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
2. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
3. die Zwecke der Verarbeitung;
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
5. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
6. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
7. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
8. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
9. Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:
10. den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
11. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
12. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
13. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
14. Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
15. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
16. Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschliessßt.