Verarbeitungstätigkeit (VT) - Erfassung

Infos zur Verarbeitungstätigkeit und zum Erfasser des Dokuments[1]

Datum der Erfassung: _____
Bearbeiter/in, Erfasser/in[2]: _____
Telefon, eMail des/der Erfassers/in: _____
_____

Kurz-Bezeichnung der Verarbeitung: _____
Übergeordneter Geschäftsprozess[3]: _____
Version[4]: _____
Beginn der Verarbeitung[5]: _____

☐ (erstmalige) Erstellung einer (neuen) Verarbeitung
☐ Änderung einer bestehenden Verarbeitung (neue Version)
☐ Abmeldung einer bestehenden Verarbeitung

Fachbereich der VT: _____
Geprüft von: _____
Geprüft am[6]: _____

[1] Diese erste Seite ist nur dann wesentlich relevant, wenn mehrere Personen in Ihrem Unternehmen diese Verarbeitungstätigkeiten erfassen.

[2] Geben Sie hier den Erfasser an. Dies dient intern für Sie als Rückfragen-Kontakt.

[3] Wenn zu einem Geschäftsprozess mehrere Verarbeitungsschritte bzw. Verarbeitungstätigkeiten gehören, können diese hiermit zugeordnet werden (dies ist meist der Fall, wenn ein Gesamt-Prozess sehr umfangreich ist und zur besseren Erfassung im Verzeichnis der Verarbeitungstätigkeiten in mehrere Einzel-Prozesse zerlegt wird).

[4] Die erstmalige Erfassung trägt wahrscheinlich die Versionsnummer 1; wenn in der Zukunft diese Verarbeitungstätigkeit überarbeitet wird, kann dies mittels Versionsnummer nachverfolgt werden.

[5] Geplanter oder tatsächlicher Beginn der Verarbeitung; kann auch das aktuelle Datum sein, wenn die Verarbeitung bereits erfolgt (und der Beginn in der Vergangenheit liegt)

[6] Die Prüfung erfolgt nach Erfassung; nach der Prüfung kann diese Verarbeitungstätigkeit in das Verzeichnis der Verarbeitungstätigkeiten (VdV als Excel) aufgenommen werden.

Beschreibung der Verarbeitung[7]:

[Information zur Langtext-Beschreibung: Gehen Sie so vor, als würden Sie einer/einem neuen Mitarbeiter/in diese (Verarbeitungs-) Tätigkeit erklären, damit diese/r diese Tätigkeit danach selbständig ausführen könnte. Gehen Sie dabei Schritt für Schritt vor, bezeichnen Sie die verwendeten (technischen) Hilfsmittel (wie Aktenordner XY, Ablagesystem XY oder Software XY) und dokumentieren Sie jeden Handgriff. Die weiteren Ausfüll-Schritte auf den nächsten Seiten vervollständigen das Dokument]

[7] Beschreiben Sie hier die Verarbeitung in Ihren Worten, um grundlegend die Verarbeitungstätigkeit nachvollziehen zu können. Dies dient zur Überprüfung, ob alles berücksichtigt wurde, bzw. dient einem externen Prüfer/Berater als Basis

Rechtmäßigkeit der Verarbeitung

Rechtsgrundlage der Verarbeitung[8]:

- ☐ Vertragserfüllung[9]
- ☐ rechtliche Verpflichtung[10]
- ☐ lebenswichtiges Interesse[11]
- ☐ öffentliches Interesse, Ausübung öffentlicher Gewalt[12]
- ☐ berechtigtes Interesse des Verantwortlichen oder Dritten[13]
- ☐ gegebene Einwilligung[14]

Beruht die Rechtmäßigkeit der Verarbeitung auf eine Vertragserfüllung, Benennung der Vertragsanbahnung oder des Vertrages[15]:

_____

_____

_____

_____

Beruht die Rechtmäßigkeit der Verarbeitung auf eine rechtliche Verpflichtung, Angabe der speziellen gesetzlichen Regelung[16]:

Name des Gesetzes (Gesetzblatt):

_____

Paragraf/Absatz/Ziffer

_____

[8] Auf welcher rechtlich legitimierten Basis gem. Art. 6 DSGVO bzw. §1 DSG (vgl. Anmerkungen und Erwägungsgründe) erfolgt die Verarbeitung?

[9] zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen (auf Anfrage der betroffenen Person) erforderlich (zB: Angebotslegung, Bewerbungen, einmalige Zusendung von Informationsmaterial, ...)

[10] zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (zB: Rechnungslegung, Lohnverrechnung, ...)

[11] erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (meist im medizinischen Bereich)

[12] Zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

[13] Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.
→ Achtung: Prüfen Sie die Grundrechte und Grundfreiheiten der betroffenen Personen, die durch Ihr berechtigtes Interesse eventuell „ausgehebelt“ würden.

[14] Gibt es keine andere Rechtmäßigkeit, ist die Einwilligung der betroffenen Person zwingend notwendig! ACHTUNG: Prüfen Sie die Einwilligungserklärung, ob diese den Vorgaben der DSGVO entspricht!

[15] Zur Sicherstellung, ob es sich tatsächlich um eine Vertragserfüllung handelt, und ob die verwendeten und verarbeiteten Daten tatsächlich dafür erforderlich sind, beschreiben Sie die Grundlage.

[16] Die Nennung der rechtlichen Bestimmung hat den Vorteil, dass bei zukünftigen Veränderungen der Gesetzesbestimmung etwaige Änderungsnotwendigkeiten in der Verarbeitungstätigkeit erkannt und erfasst werden können.

Beruht die Rechtmäßigkeit der Verarbeitung auf eine übertragene Aufgabe im öffentlichen Interesse, Bezeichnung/Beschreibung der Aufgabe und Nennung des Auftraggebers[17]:

Auftraggeber:

_____

Beschreibung des Auftrags

_____

_____

_____

Beruht die Rechtmäßigkeit der Verarbeitung auf das berechtigte Interesse des Verantwortlichen oder eines Dritten, Nennung der Begründung[18]:

_____

_____

_____

Beruht die Rechtmäßigkeit der Verarbeitung auf eine Einwilligung, Nennung der Einwilligungsklausel und den Einwilligungsmechanismus[19]:

_____

_____

_____

[17] Die Nachverfolgung soll auf einfachem Wege gewährleistet werden. Geben Sie hier die notwendigen Informationen bekannt.

[18] Achten Sie bei der Begründung auf die Abwägung gegenüber den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person – **lassen Sie diese gegebenenfalls juristisch prüfen**!

[19] Wie lautet der Einwilligungstext und wann, wie und wo wird dieser zur Unterfertigung vorgelegt?

Von wem wurden die Daten erhoben (wichtig für Informationspflichten)?

Wie sind Sie zu diesen Daten gelangt?

☐ Daten selbst erhoben (direkt bei der betroffenen Person)

☐ Daten von Dritten übermittelt bekommen

Wenn Sie die personenbezogenen Daten selbst erhoben haben, wie, wo und wann haben Sie den betroffenen Personen die Pflichtinformation über die Datenverarbeitung zugänglich gemacht[20]?

Beschreibung der Informationspflicht

_____

_____

_____

_____

_____

_____

Wenn Sie die personenbezogenen Daten von Dritten übermittelt bekommen haben, von wem und wie und wo haben Sie die Daten erhoben oder erhalten? Wie, wo und wann haben Sie den betroffenen Personen die Pflichtinformation über die Datenverarbeitung zugänglich gemacht[21]?

Beschreibung der Informationspflicht

_____

_____

_____

_____

_____

_____

_____

_____

_____

[20] Art. 13 DSGVO regelt die Informationspflicht des Verantwortlichen ggü. den betroffenen Personen, wenn der Verantwortliche die Daten direkt bei der betroffenen Person erhebt.

[21] Art. 14 DSGVO regelt die Informationspflicht des Verantwortlichen ggü. den betroffenen Personen, wenn der Verantwortliche die Daten nicht bei der betroffenen Person erhebt, sondern diese von einem Dritten übermittelt bekommen hat.

Personenbezogene Daten und betroffene Personen

Kreis der betroffenen Personen (betroffene Personengruppe) [22]:

_____

_____

_____

Verwendete Datenarten (erfassen Sie konkret die verwendeten/verarbeiteten Datenarten) [23]:

_____

_____

_____

Verwendete (sensible) Datenarten der besonderen Kategorien gem. Art. 9 DSGVO [24]:

_____

_____

_____

Verwendete sonstige Daten (die Sie eventuell noch nicht konkret zuordnen können) [25]:

_____

_____

_____

[22] Nennen Sie die Personengruppen bzw. den Kreis der betroffenen Personen wie Mitarbeiter, Kunden, Gäste, Lieferanten, Schuldner, Patienten, Versicherungsnehmer, Interessenten, Messebesucher, ... Segmentieren Sie dabei so weit wie unbedingt nötig und halten Sie die Anzahl der verschiedenen Personengruppen so gering wie möglich. Eventuell werden Sie erst bei Prüfung aller erfassten Tätigkeiten die endgültige Definition der einzelnen notwendigen Personengruppe entscheiden können.

[23] Eine beispielhafte Liste der Datenarten ist im Dokument „***Appendix-A_Datenarten***“ enthalten.

[24] Erfassen Sie Gesundheitsdaten (zB. Sozialversicherungsnummer, Unverträglichkeiten, Gesundheitszustände, ...), biometrische Daten (zB. Fingerprint für Zutrittssysteme, Bilddaten von Mitarbeitern oder Kunden, ...), Religionsdaten (Religionszugehörigkeit zB. für Lohnverrechnung und Berücksichtigung etwaiger zusätzlicher Feiertage), ... Eine Liste der besonderen Kategorien und beispielhafte Nennung der Datenarten finden Sie im Dokument „***Appendix-A_Datenarten***“

[25] Erfassen Sie auch sonstige verwendete Daten in dieser Verarbeitung, da eventuell im Zuge einer Folgenabschätzung erst im Zusammenhang erkennbar wird, welche Auswirkung eine Veröffentlichung solcher Daten nach sich ziehen könnten.

Datenweitergabe und Empfänger[26]

An welche Empfänger werden Daten weitergegeben bzw. übermittelt?

(Interne) Empfänger innerhalb der Sphäre des Verantwortlichen[27]:

Dazu gehören insbesondere auch Auftragsverarbeiter, mit denen ein entsprechender Auftragsverarbeiter-Vertrag abzuschließen ist!

Kopieren Sie die nachfolgenden Zeilen, so oft diese benötigt werden.

Bezeichnung des Empfängers: _____

Zweck der Übermittlung: _____

Datenarten: _____

Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzern-Unternehmen)[28]:

Kopieren Sie die nachfolgenden Zeilen, so oft diese benötigt werden.

Bezeichnung des Empfängers: _____

Zweck der Übermittlung: _____

Datenarten: _____

(geplante) Übermittlung an Drittstatten (außerhalb der EU)[29]:

Kopieren Sie die nachfolgenden Zeilen, so oft diese benötigt werden.

Bezeichnung des Drittstaates: _____

Zweck der Übermittlung: _____

Datenarten: _____

_____

_____

[26] „Empfänger" ist jede Person oder Stelle, die Daten erhält, z. B. Vertragspartner, Kunden (zB Daten von Kooperationspartnern), Behörden, Versicherungen, ärztliches Personal, Auftragsverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter/-entsorger), oder ein Verfahren bzw. Geschäftsprozess, an den Daten weitergegeben werden.

[27] zB: IT-Dienstleister (der theoretisch Zugriff auf alle Daten hat), Software-Hersteller (Branchenlösungen, CRM, ERP, ...), eMail-Provider (Google, Microsoft, ...), Lohnverrechnung, Buchhaltung, Steuerberater, ...

[28] Für die Datenweitergabe an Dritte ist in Folge eventuell eine explizite Zustimmung der betroffenen Person notwendig. Für gesetzlich vorgeschriebene Übermittlung ist keine Zustimmung erforderlich (zB: GKK, Finanz).

[29] Übermittlung an Drittstaaten außerhalb der EU ist gesondert zu prüfen: besteht ein so genannter Angemessenheitsbeschluss, so kann die Datenübermittlung wie eine Übermittlung innerhalb der EU angesehen werden. (Liste der Länder mit Angemessenheitsbeschluss = anerkannte Drittländer: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Internationaler-Datenverk.html).
Liste der US-Unternehmen, die sich dem Privacy-Shield unterwerfen: https://www.privacyshield.gov/participant_search

Übermittlungssysteme

Geben Sie die verwendeten Übermittlungssysteme an [30]:

Übermittlung Eingang:

_____
_____
_____
_____
_____
_____

Übermittlung Ausgang:

_____
_____
_____
_____
_____
_____

[30] zB: eMail, Telefon, Fax, Post/Zustellservice, Persönlich, Messengerdienste, Homepage

Mittel der Verarbeitung (eingesetzte Software oder verwendete Systeme)

Führen Sie nachstehend jede eingesetzte Software und jedes verwendete System an[31]:

Kopieren Sie die nachfolgenden Zeilen, so oft diese benötigt werden.

Bezeichnung und Hersteller: ____

Bereitstellung:

☐ Eigenentwicklung / Individualsoftware

☐ Standard- bzw. Kauf-Software

☐ Cloud-Service

Funktionsbeschreibung:

Beschreibung der Funktionen, Arbeitsweise(n) und Einsatzweise des Systems

____

____

____

Bezeichnung und Hersteller: ____

Bereitstellung:

☐ Eigenentwicklung / Individualsoftware

☐ Standard- bzw. Kauf-Software

☐ Cloud-Service

Funktionsbeschreibung:

Beschreibung der Funktionen, Arbeitsweise(n) und Einsatzweise des Systems

____

____

____

Bezeichnung und Hersteller: ____

Bereitstellung:

☐ Eigenentwicklung / Individualsoftware

☐ Standard- bzw. Kauf-Software

☐ Cloud-Service

Funktionsbeschreibung:

Beschreibung der Funktionen, Arbeitsweise(n) und Einsatzweise des Systems

____

____

____

[31] Mit welchen Mitteln verarbeiten Sie die personenbezogenen Daten? Geben Sie alle Systeme bekannt, zB: Aktenordner (Papier), Kontaktdatenbank, Faktura-Programm, Branchen-Software-Lösung, Warenwirtschaftsprogramm, File-Server, PC, Mailprogramm, Newsletter-Programm, diverse Cloud-Dienste, Mobiltelefon, ...

Zwecke der Verarbeitung

Zweck(e) der Verarbeitung / Zweckbestimmung der Datenverarbeitung:

____

____

____

Zugriffsberechtigungen

Wer hat in Ihrem Unternehmen Zugriff auf die Daten in dieser Verarbeitungstätigkeit? Geben Sie die Benutzerrollen an (zB. Geschäftsführung, Einkauf, Vertrieb, Marketing, ...)

Führen Sie nachstehend jede zugriffsberechtigte Personengruppe an[32]:

Bezeichnung Personengruppe: ____

Berechtigungsrolle: ____

Zugriff auf folgende Datenarten: ____

Art des Zugriffs:
- ☐ Lesen
- ☐ Schreiben
- ☐ Löschen

Zweck/Grund des Datenzugriffs: ____

Bezeichnung Personengruppe: ____

Berechtigungsrolle: ____

Zugriff auf folgende Datenarten: ____

Art des Zugriffs:
- ☐ Lesen
- ☐ Schreiben
- ☐ Löschen

Zweck/Grund des Datenzugriffs: ____

Bezeichnung Personengruppe: ____

Berechtigungsrolle: ____

Zugriff auf folgende Datenarten: ____

Art des Zugriffs:
- ☐ Lesen
- ☐ Schreiben
- ☐ Löschen

Zweck/Grund des Datenzugriffs: ____

[32] Geben Sie alle Personengruppen getrennt an.

Aufbewahrungs- bzw. Löschfristen der Daten

Die Datenverarbeitung unterliegt eventuell gesetzlich geregelter oder normierter[33] Aufbewahrungsfristen.

Gesetzliche Regelungen: _____
Bezeichnung des Gesetzes: _____
Detailinformation: _____

Normen-Vorgaben: _____
Bezeichnung der Norm: _____
Detailinformation: _____

Auf Basis der geregelten Aufbewahrungsfrist, kann dann die entsprechende früheste Löschfrist definiert werden:

Regellöschfrist: ob, wann, nach welchen Regeln werden die Daten gelöscht

- ☐ 7 Jahre zwecks Buchhaltung / Lohnverrechnung
- ☐ 30 Jahre (Arbeitszeugnisse, Gewährleistung)
- ☐ 50 Jahre (zB Gesundheitswesen, Gutachten, ...)
- ☐ 6 Monate (Bewerberdaten)
- ☐ sofort, da kein Bedarf
- ☐ Nach Auftragserfüllung
- ☐ nach _____ Jahren, weil _____

Profiling[34]

Führen Sie eine automatisierte Bewertung, Analyse oder Vorhersage auf Basis der verarbeiteten personenbezogenen Daten durch?

☐ Ja ☐ Nein

Bei JA, geben Sie nähere Details und die Begründung zum Verfahren an:

_____

[33] Diverse ISO-Zertifizierungen oder andere Organisations- oder Management-Zertifizierungen schreiben eigene Aufbewahrungsfristen für Dokumente oder Dokumentationen vor. Erfassen Sie lückenlos alle Vorgaben zur Aufbewahrungsfrist der Daten aus dieser Verarbeitungstätigkeit.

[34] Mit Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten gemeint, die darin besteht, die Daten dahingehend zu verwenden, um persönliche Aspekte (Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort und Ortswechsel) einer betroffenen Person zu bewerten, zu analysieren oder vorherzusagen. Dies betrifft vor allem, aber nicht nur, die Bereiche Web-Analytics, Affiliate-Marketing, Zutrittskontrollsysteme und vieles mehr. Beispiel: Ein Online-Kredit- oder Leasing-Rechner führt im Hintergrund automatisiert eine Bonitätsprüfung durch und bereitet auf Basis des Ergebnisses den Vertrag automatisiert vor (mit entsprechend höheren oder niedrigeren Zinsen). Diese automatisierte Entscheidungsfindung hat eine rechtswirksame Auswirkung auf den Kunden.

TOM (technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit)[35]

Wurde eine Risikoanalyse durchgeführt ☐ Ja (kurze Ergebnis-Beschreibung)
☐ Nein, Begründung, weshalb nicht

_____
_____
_____

Wurden Maßnahmen (auf Basis §54 DSG) zur Datensicherheit getroffen?

Zugangskontrolle: ☐ Ja (kurze Beschreibung der Maßnahmen)
☐ Nein, Begründung, weshalb nicht

_____
_____
_____

Datenträgerkontrolle: ☐ Ja (kurze Beschreibung der Maßnahmen)
☐ Nein, Begründung, weshalb nicht

_____
_____
_____

Speicherkontrolle: ☐ Ja (kurze Beschreibung der Maßnahmen)
☐ Nein, Begründung, weshalb nicht

_____
_____
_____

Benutzerkontrolle: ☐ Ja (kurze Beschreibung der Maßnahmen)
☐ Nein, Begründung, weshalb nicht

_____
_____
_____

Zugriffskontrolle: ☐ Ja (kurze Beschreibung der Maßnahmen)

[35] Anmerkungen und eine Erklärung zur Datensicherheit finden Sie im Dokument „***Appendix-B_Datensicherheit***“. Sie können die technischen & organisatorischen Maßnahmen auch einmal zentral erfassen (statt explizit zu jeder Verarbeitungstätigkeit), sofern diese Ihr Unternehmen betreffen oder auf alle Verarbeitungstätigkeiten gleichsam zutreffen. Abweichungen oder Sonderregelungen führen Sie bei der entsprechenden Verarbeitungstätigkeit hier an.

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Übertragungskontrolle:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Eingabekontrolle:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Transportkontrolle:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Wiederherstellung:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Zuverlässigkeit:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

_____

_____

Datenintegrität:

☐ Ja (kurze Beschreibung der Maßnahmen)

☐ Nein, Begründung, weshalb nicht

_____

Backup-Regelung: [Information seitens IT-Betreuung einbinden]

Beschreiben Sie das Backup-Konzept und geben Sie an, ab wann spätestens nach Löschung der Daten diese auch aus sämtlichen Backups entfernt sind

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design / Privacy by Default)[36]

Sind die Grundsätze eingehalten? ☐ Ja
☐ Nein, Begründung, weshalb nicht

Datenübertragbarkeit

Ist eine Datenübertragbarkeit gegeben, das heißt, besteht eine Möglichkeit, die personenbezogenen Daten an die betroffene Person in einem gängigen, standardisierten und maschinenlesbaren Format zu übermitteln?

☐ Ja (wodurch?) ☐ Nein, Begründung, weshalb nicht

[36] Gem. Art. 25 DSGVO sind Maßnahmen zu ergreifen, um Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen (Privacy by Design) sowie durch Voreinstellung sicher zu stellen, dass grundsätzlich nur unbedingt zum Verarbeitungszweck erforderliche Daten verarbeitet werden (Privacy by Default).

DISCLAIMER und Verwendungshinweise

Die Autoren (Ing. Dipl.-Ing.(FH) Harald Schenner, CMC und Dipl.-Ing. Gerald Kortschak, BSc CMC) weisen ausdrücklich darauf hin, dass die hier vorliegende Unterlage nach Treu und Glauben angefertigt und im Wesen den Inhalt der aktuellen Gesetzgebung wiedergibt, jedoch keine juristische Beratung durch einen eingetragenen Rechtsanwalt ersetzt.

Sie erreichen die Autoren unter www.derSchenner.at bzw. www.sevian7.com oder unter der gemeinsamen Projektseite www.dsgvo2018.at.

Die Autoren sind zertifizierte Datenschutz-Experten, zertifizierte IT-Security-Experten und zertifizierte Unternehmensberater. Beide unterrichten auf Fachhochschulen und sind Trainer bei Wifi, Incite und weiteren Bildungsträgern.

CERTIFIED DATA & IT SECURITY EXPERT

CMC

CERTIFIED DIGITAL CONSULTANT

WIR NEHMEN **WISSEN** IN BETRIEB.