



Summereder Aigner Rechtsanwaltsgesellschaft m.b.H.
RA Mag. Philipp Summereder
RA Mag. Susanne Aigner

Beilage zum Verzeichnis der Verarbeitungstätigkeiten

Das zur Verfügung gestellte Musterkonzept für ein umfassendes Verzeichnis der Verarbeitungstätigkeiten soll als Anregung dienen, wie ein eigenes Verzeichnis der Verarbeitungstätigkeiten gestaltet werden kann und erweitert die jedenfalls gem. Art. 30 EU-DSGVO notwendigen Angaben um einige weitere Textfelder, die bei der gesamtheitlichen Umsetzung der Herausforderungen der EU-DSGVO gemäß dem im Zuge der branchenspezifischen Workshops präsentierten Vorgehensweise unterstützen.

Die vorausgefüllten Textbausteine sind als Beispiele und Muster zu verstehen und bedürfen jedenfalls einer Kontrolle, Korrektur und Ergänzung des jeweiligen Verantwortlichen unter Berücksichtigung der jeweiligen Besonderheiten im eigenen Betrieb. Als Grundlage für die beispielhafte Befüllung wurde die Standard- und Musterverordnung 2004 herangezogen und diese um in Unternehmen beispielhaft vorhandene Verarbeitungstätigkeiten ergänzt, die jedoch je nach Berufsgruppe und Unternehmen noch erweitert werden müssen.

Die vorliegende Erläuterung zum Musterkonzept für ein Verzeichnis der Verarbeitungstätigkeiten soll einerseits einen kurzen Überblick über die Begrifflichkeiten der EU-DSGVO bieten und andererseits als Unterstützung bei der rechtsrichtigen Gestaltung des Verzeichnisses dienen. Für die Vollständigkeit und Richtigkeit des zur Verfügung gestellten Musters wird keine Haftung übernommen.

Begriffsbestimmungen

Zur Gestaltung des Verzeichnisses der Verarbeitungstätigkeiten ist es notwendig, die wesentlichen Begrifflichkeiten der EU-DSGVO präsent zu haben. Sämtliche Begriffsbestimmungen im Gesetzeswortlaut finden Sie auch unter Art. 4 der EU-DSGVO.

„personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Dies bedeutet, dass neben Namen und Adressdaten auch etwa GPS-Daten, Benutzerkennzeichen (Logindaten), Fotos oder Fingerabdrücke personenbezogene Daten darstellen.

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ord-

nen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Dabei ist wesentlich, dass sowohl (manche) analoge als auch digitale Verarbeitung vom Umfang der EU-DSGVO umfasst ist. So sind auch Verarbeitungen wie das Anlegen von (physischen) Ordnern oder die Archivierung alter Daten im Keller Verarbeitungsvorgänge, die von der EU-DSGVO umfasst sind.

„Verantwortlicher“ bezeichnet 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

In diesem Zusammenhang ist also insbesondere bei der Gestaltung des Verzeichnisses der Verarbeitungstätigkeiten nach dem Verantwortlichen im Sinne der EU-DSGVO (dies ist zumeist die juristische Person / das Unternehmen, für das das Verzeichnis gestaltet wird) und dem für die Befüllung innerhalb dieses Betriebs zuständigen Mitarbeiter zu unterscheiden. Letzterer ist nicht „Verantwortlicher“ im Sinne der EU-DSGVO.

Der Verantwortliche unterscheidet sich vom Auftragsverarbeiter dadurch, dass er selbst über die Art, den Umfang, die Umstände und den Zweck der Verarbeitung der Daten entscheidet, während der Auftragsverarbeiter Daten grundsätzlich nur auf Weisung des Verantwortlichen verarbeitet.

„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Klassische Auftragsverarbeiter sind beispielsweise IT-Unternehmen, die Mailingsysteme, Serverleistung oder vergleichbare Dienstleistungen anbieten.

„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

Empfänger sind sohin all jene Personen oder Einrichtungen, denen Daten tatsächlich übersandt werden, aber auch solche, denen beispielsweise im Rahmen von Fernwartung oder eines Zugriffsberechtigungsmanagements Einsicht in Daten ermöglicht wird.

Gesetzliche Grundlage für das Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen

Art. 30 EU-DSGVO

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- b) die Zwecke der Verarbeitung;
- c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- e) 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;
- f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Seitens der österreichischen Datenschutzbehörde wurde keine ausdrückliche Empfehlung abgegeben, wie ein Verzeichnis der Verarbeitungstätigkeiten auszusehen hat, es wurde jedoch angemerkt, dass man sich am nach der Rechtslage des DSG 2000 bestehenden Datenverarbeitungsregister orientieren kann.

Dementsprechend ist zur Konzeptionierung des Musterkonzepts für ein Verzeichnis der Verarbeitungstätigkeiten als Grundlage die sog. Standard- und Musterverordnung 2004 herangezogen worden, die nach der bis zum 25.05.2018 geltenden Rechtslage einen Überblick darüber gibt, welche Struktur der österreichische Gesetzgeber selbst für die Beschreibung von Verarbeitungstätigkeiten (vormals Datenanwendungen) vorgibt.

Die Gestaltung des Verzeichnisses der Verarbeitungstätigkeiten

Um eine vollständige und richtige Gestaltung des VdV mit bestimmten Verarbeitungstätigkeiten zu gewährleisten, ist es hilfreich, sich die Prozesse und den Datenfluss innerhalb der Abteilungen eines Unternehmens genau durchzudenken.

Eruieren Sie, welche Daten über welche Personengruppen (Kategorien betroffener Personen) erfasst und verarbeitet werden, wie diese zu Ihnen gelangen, wie sie innerhalb der Organisation gespeichert bzw. verarbeitet und an wen sie weitergegeben werden. Durch das Aufzeichnen entsprechender Prozesse ist einfach zu erkennen, wie eine Verarbeitungstätigkeit ins Register aufgenommen werden kann.

Für den Fall, dass in Ihrer Organisation zahlreiche Verarbeitungstätigkeiten vorgenommen worden, ist es empfehlenswert, neben einer Gesamtübersicht über alle Verarbeitungstätigkeiten ein eigenes Excel-Blatt für jede Verarbeitungstätigkeit anzulegen, um dort weitere relevante Informationen zu erfassen.

Bestehende und formatierte Excelblätter kann man vervielfältigen, indem man am Fußende der Tabelle auf den zugehörigen Reiter rechtsklickt, und dann unter den zur Verfügung stehenden Optionen das Feld „Verschieben oder Kopieren“ wählt. Dort ist das zu kopierende Tabellenblatt auszuwählen und beim Feld „Kopie erstellen“ ein Haken zu setzen. Mit einem Klick auf OK ist das Tabellenblatt kopiert. Am „Ende“ Ihres Musterverzeichnisses finden Sie ein bereits formatiertes aber gänzlich unbefülltes Tabellenblatt mit der Angabe „00“ am Reiter des Tabellenblattes. Dieses eignet sich dafür, mehrfach kopiert und zur Befüllung herangezogen zu werden.

1. Als Verarbeitungstätigkeit kann dabei immer eine Aufgabe oder ein Prozess einer bestimmten Abteilung Ihres Unternehmens verstanden werden, in deren/dessen Zuge personenbezogene Daten verarbeitet werden. So wurden als Verarbeitungstätigkeiten beispielsweise das Rechnungswesen, die Personalverwaltung, das Marketing, oder aber auch das Verwalten von Benutzerkennzeichen, die Videoüberwachung oder vergleichbare Vorgänge bezeichnet.

Aus dieser vom Gesetzgeber im Rahmen der bisherigen Rechtslage vorgenommenen Kategorisierung sind zwei wesentliche Dinge ersichtlich. Zum einen, dass Verarbeitungstätigkeiten durchaus als Überkategorie verschiedene Unterkategorien zusammenfassen können.

In der Verarbeitungstätigkeit Personalverwaltung sind beispielsweise verschiedene mit der Personalverwaltung in Zusammenhang stehende Tätigkeiten wie die Arbeitszeiterfassung, die Urlaubsverwaltung oder auch das Bewerbermanagement zusammengefasst.

Bei der Formulierung einer Verarbeitungstätigkeit ist es also in einem ersten Schritt sinnvoll, den konkreten Zweck einer Datenverarbeitung anzusehen und all jene Zwischenschritte, die zur Erreichung dieses Zwecks notwendig sind, in einer Verarbeitungstätigkeit zusammenzufassen. Welcher Zweck eine bestimmte Verarbeitungstätigkeit definiert, ist immer unternehmensbezogen und individuell zu betrachten.

Unterscheiden Sie die Verarbeitungstätigkeit unbedingt von einer Applikation!

Im Zuge verschiedener Verarbeitungstätigkeiten werden oftmals verschiedenste Anwendungen / Applikationen verwendet. So benötigt man im Zuge der Personalverwaltung möglicherweise sowohl eine Lohnverrechnungssoftware, eine Software für die Zeiterfassung, möglicherweise eine Bewerberdatenbank und übermittelt verschiedenste Dinge im Zuge dieser Verarbeitung per E-Mail-Programmen oder sonstigen Applikationen und speichert Dokumente in Excel-Dokumenten.

Diese Programme / Applikationen sind für sich betrachtet bei Interpretation der Vorgaben des Gesetzgebers **keine eigenen Verarbeitungstätigkeiten**, sondern nur die Werkzeuge, die Sie zur Verarbeitung von Daten heranziehen.

2. Den Zweck der Verarbeitung kann man stets über die Aufgabe definieren, zu deren Erfüllung die Verarbeitung von Daten erfolgt. Die Standard- und Musterverordnung 2004 gibt zahlreiche Verarbeitungstätigkeiten vor und beschreibt deren Zweck, sodass sie bei der Formulierung anderer Verarbeitungstätigkeiten als Grundlage herangezogen werden kann.

3. Die Kategorien betroffener Personen stellt eine allgemeine Beschreibung der Personengruppen dar, deren Daten im Zuge der Verarbeitungstätigkeit verarbeitet werden. Eine Beschreibung dieser Kategorien kann stets in der Form erfolgen, als dass man eine geeignete Überbezeichnung anhand der Merkmale findet, die die Personengruppe, deren Daten verarbeitet werden, vereint.

Während Bezeichnungen wie „Vertragspartner“ oder „Verbraucher“ möglicherweise zu weit gefasst ist, sind Bezeichnungen wie „Bewerber“, „Kontaktpersonen“, „Interessierte“, „Kunden“ usw. geeignete Kategorien betroffener Personen.

4. Die Grundlage der Verarbeitung

Als Grundlage der Verarbeitung ist grundsätzlich einzutragen, wie die Verarbeitung dieser Daten gerechtfertigt wird. Die entsprechenden Bedingungen sind in Art. 6 EU-DSGVO geregelt. Wählen Sie den für Ihre Verarbeitung passenden Rechtfertigungsgrund aus und tragen Sie ihn in das Verzeichnis ein.

- a. Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b. die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c. die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;
- d. die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e. die Verarbeitung ist für die **Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt**, die dem Verantwortlichen übertragen wurde;

- f. die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

In diesem Zusammenhang ist es hilfreich, insbesondere den Fällen von c. und f. auch die tatsächliche gesetzliche Grundlage für die Argumentation der Verarbeitung anzugeben – dies ist hilfreich bei der Erhebung, wie lange Daten verarbeitet werden dürfen, und wann sie wieder zu löschen sind.

5. Als Kategorien personenbezogener Daten sind alle Informationen zu verstehen, die Sie über bestimmte Betroffene verarbeiten. Dazu ist es hilfreich, die zur Verarbeitung herangezogenen Applikationen (wie beispielsweise die Buchhaltungssoftware, Kommunikationsprogramme oder Excel-Dateien) danach zu durchforsten, welche Informationen zu bestimmten Personen gespeichert werden.

Vergessen Sie dabei nicht auf Informationen, die ohne Ihr Zutun systembedingt erfasst werden, wie beispielsweise Logfiles, Zeitstempel oder ähnliches, sofern diese einer bestimmten Person zurechenbar sind.

Einen Anhaltspunkt für die Erfassung dieser Kategorien kann wiederum die Standard- und Musterverordnung 2004 bieten, die in verschiedenen Beispielverarbeitungstätigkeiten zahlreiche Kategorien anführt. Grundsätzlich reicht es aus, die verarbeiteten Daten in allgemeine Gruppen zu kategorisieren, wie beispielsweise Kontaktdaten, Zahlungsdaten, Stammdaten,...

Es ist aber durchaus empfehlenswert, im Zuge der Evaluierung eine genaue Übersicht über die einzelnen verarbeiteten Datenkategorien zu erstellen, da dies in weiterer Folge eine rechtsrichtige Information (Datenschutzerklärung) und Unterstützung von Betroffenen (Auskunftsbegehren) maßgeblich erleichtern kann.

Erheben Sie auch, ob besondere Kategorien personenbezogener Daten verarbeitet werden. Besondere Kategorien sind etwa 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.

Die Verarbeitung von besonderen Kategorien pb Daten ist an besondere Rechtfertigungsgründe gekoppelt und kann weitere rechtliche Folgen nach sich ziehen. (Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung oder der Bestellung eines Datenschutzbeauftragten.)

6. In einem weiteren Schritt ist anzugeben, welche **Kategorien an Empfängern** die personenbezogenen Daten erhalten (können).

Überlegen Sie, welche Institutionen/Unternehmen/Kooperationspartner oder sonstige Dritte Daten erhalten können – und behalten Sie dabei im Blick, dass auch die Gewährleistung einer Einsicht dazu führt, dass jemand Daten empfängt.

Auch hier bietet sich an, die verschiedenen Empfänger der Standard- und Musterverordnung zu prüfen und allenfalls zu ergänzen.

7. Bitte erfassen Sie, ob eine **Übermittlung von personenbezogenen Daten ins Drittland erfolgt – und wenn ja, in welche Länder. In einem ersten Schritt sind nur die einzelnen Länder, also Empfängerländer außerhalb der Europäischen Union und des EWR, anzugeben. Die Angabe von „geeigneten Garantien o.ä.“ sollte in Zusammenarbeit mit einem Experten erfolgen.**

8. Fristen für die Löschung

Personenbezogene Daten dürfen nur solange aufbewahrt werden, solange eine Grundlage (siehe Punkt 4.) besteht, danach müssen sie gelöscht werden. In diesem Feld sind die Kriterien anzugeben, nach denen sich die Fristen für die Aufbewahrung richten.

Im Idealfall sollten Sie für die Umsetzung in Ihrem eigenen Unternehmen, sofern möglich, tatsächlich auch konkrete Angaben zu der Speicherdauer erfolgen; dies unterstützt Sie auch dabei, eine Löschroutine im Betrieb zu entwickeln.

9. Technische/organisatorische Maßnahmen

In diesem Zusammenhang ist anzugeben, wie die verarbeiteten Daten durch technische und organisatorische Maßnahmen gem. Art. 32 EU-DSGVO geschützt werden. Es macht in kleineren und mittleren Unternehmen oft Sinn, diese Angaben für sämtliche Verarbeitungstätigkeiten oder Gruppen von Verarbeitungstätigkeiten zu vereinheitlichen. Dieses Feld sollte also derjenige befüllen, der in einer Organisation (Unternehmen/Gebietskörperschaft) für die Implementierung und Aufrechterhaltung dieser technischen und organisatorischen Maßnahmen zuständig ist.

10. Verwendete Applikation(en)

Es ist gesetzlich nicht erforderlich, aber für weitere Aufgaben im Zusammenhang mit der EU-DSGVO hilfreich, die zur Verarbeitung der Daten herangezogenen Applikationen (Software, Programme,...) anzugeben. Dadurch gewinnen Sie einerseits einen Überblick darüber, wo überall nach „Kategorien personenbezogener Daten“ oder „Empfängerkategorien“ gesucht werden kann; zudem werden in weiterer Folge Prozesse bei der Beantwortung von Anfragen Betroffener oder bei der Einrichtung einer Löschroutine erleichtert.

Die übrigen Felder dienen dazu, innerhalb Ihrer Organisation Zuständigkeiten zu erfassen und zu dokumentieren. Sie können bei Bedarf befüllt werden.

Die vorliegende Information soll dazu dienen, Ihnen die Gestaltung Ihres Verzeichnisses der Verarbeitungstätigkeiten zu erleichtern, kann allerdings den prüfenden Blick eines Experten nicht ersetzen. Nachdem die in Ihrer Organisation vorhandenen Verarbeitungstätigkeiten erfasst wurden, ist daher eine gemeinsame Erörterung und Finalisierung mit einem Datenschutzspezialisten anzuraten.