D2 Verarbeitungstätigkeiten

Die DS-GVO verwendet „Verarbeitungstätigkeit“ in Art. 30 DS-GVO als zentralen Begriff des Datenschutzmanagements und definiert den Begriff der „Verarbeitung“ in Art. 4 Abs. 2 DS-GVO:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck (...) Verarbeitung 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 Ordnen, 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; (...).“

Art. 30 DS-GVO listet die Angaben auf, die in das Verzeichnis der Verarbeitungstätigkeiten, das vom Verantwortlichen oder Auftragsverarbeiter zu führen ist, aufzunehmen sind. Genannt werden dort u. a.:

- Namen und Kontaktdaten des Verantwortlichen, des Vertreters sowie des Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen, personenbezogener Daten und Empfänger sowie ggfs. die Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation,
- die vorgesehenen Fristen für die Löschung,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO.

Diese allgemeine Beschreibung einer Verarbeitung stellt noch keine ausreichende Dokumentation von Verarbeitungstätigkeiten dar und erfüllt allein noch nicht die Anforderungen an Transparenz gemäß Art. 5 Abs. 2 DS-GVO.

Die Funktion der vollständigen Dokumentation einer Verarbeitung besteht darin, dass alle relevanten Komponenten einer Verarbeitungstätigkeit aufgrund der bestehenden Rechenschaftspflicht prüffähig sind, um diese einer datenschutzrechtlichen Beurteilung unterziehen zu können. Prüffähigkeit bedeutet dabei, dass die Funktionen aller Komponenten, die bei einer Verarbeitungstätigkeit zum Einsatz kommen, insbesondere die Komponenten auf der Ebene der elektronischen Datenverarbeitung und Kommunikation, einer Soll-Ist-Bilanzierung zugänglich sind.

Diese Prüfbilanz bezüglich funktionaler Eigenschaften sowie der getroffenen technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit muss dann wiederum einer rechtlichen Beurteilung der Rechtskonformität bzw. Ordnungsmäßigkeit insgesamt unterzogen werden können unter der Fragestellung, ob die richtigen Maßnahmen zweckgemäß ausgewählt und mit der korrekten Wirkintensität betrieben werden.

D2.1 Ebenen einer Verarbeitung oder Verarbeitungstätigkeit

Um eine personenbezogene Verarbeitung vollständig zu erfassen, hat es sich bewährt, bei der Gestaltung oder Prüfung von Verarbeitungstätigkeiten zumindest drei verschiedene Ebenen der Darstellung wesentlicher Einflussgrößen oder Bestandteile zu unterscheiden. Wesentlich ist das Verständnis, dass eine „Verarbeitungstätigkeit“ bspw. nicht deckungsgleich mit der Verwendung einer

bestimmten Technik oder eines bestimmten Fachprogramms ist.

Auf der **Ebene 1** ist eine personenbezogene Verarbeitung im datenschutzrechtlichen Sinne angesiedelt. Diese Verarbeitung findet bspw. im Rahmen eines privatrechtlich agierenden Unternehmens oder einer Behörde, die dem öffentlichen Recht unterliegt, statt, für deren Aktivitäten der Verantwortliche verantwortlich ist. Diese Ebene entspricht dem, was vielfach als ein „Fachverfahren“ und „Geschäftsprozess“ mit einem bestimmten funktionalen Ablauf der Verarbeitungstätigkeit verstanden wird. Auf dieser Ebene des Verständnisses einer Verarbeitung werden die für eine Verarbeitungstätigkeit erforderlichen personenbezogenen Daten sowie die gesetzlichen Anforderungen bestimmt. Der Verantwortliche definiert entsprechende Rollen und Berechtigungen an den personenbezogenen Daten und bestimmt die zu verwendenden IT-Systeme und Prozesse. Wesentlich für die datenschutzrechtlich angemessen funktionale Gestaltung dieser Ebene ist die **Bestimmung des Zwecks** oder der Zwecke der Verarbeitungstätigkeit.

Auf der **Ebene 2** ist die praktische Umsetzung der Verarbeitung und des Zwecks angesiedelt. Diese umfasst zum einen in der Regel die Rolle der Sachbearbeitung sowie die IT- Applikation(en), die sich genauer auch als „Fachapplikation eines Fachverfahrens“ bezeichnen lässt. Die Sachbearbeitung und die Fachapplikation müssen die funktionalen und (datenschutz-)rechtlichen Anforderungen, denen die Verarbeitung unterliegt, vollständig erfüllen. Die **Fachapplikation muss die Zweckbindung sicherstellen**. Die Applikation muss die Verarbeitung zusätzlicher Daten oder zusätzliche Verarbeitungsformen ausschließen, selbst wenn sie funktional besonders komfortabel sein mögen. Damit soll das Risiko minimiert werden, dass sie die Zweckbindung unterlaufen oder der Zweck überdehnt wird.

Auf der **Ebene 3** ist die IT-Infrastruktur angesiedelt, die Funktionen bereitstellt, die eine Fachapplikation der Ebene 2 nutzt. Zu dieser Ebene an „technischen Services“ zählen Betriebssysteme, virtuelle Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme wie SAN oder NAS, CPU- Cluster, sowie die Kommunikationsinfrastruktur einer Organisation wie das Telefon, das LAN, der Internetzugang oder der Betrieb von Webseiten. Auch hier gilt, dass diese Systeme innerhalb einer Verarbeitungstätigkeit jeweils so zu gestalten und zu nutzen sind, dass die **Zweckbindung erhalten** bleibt. Damit die Zweckbindung bzw. Zwecktrennung auf dieser Ebene durchgesetzt werden kann, müssen typischerweise technische und organisatorische Maßnahmen getroffen werden.

D2.3 Komponenten einer Verarbeitung oder Verarbeitungstätigkeit

Aus den Vorgaben der Datenschutz-Grundverordnung ergeben sich unmittelbar die Komponenten Daten, Systeme und Dienste. Bei der konkreten Modellierung von Verarbeitungstätigkeiten mit Personenbezug ist es jedoch notwendig, die folgenden drei Komponenten zu betrachten:

1. die personenbezogenen **Daten**,
2. die beteiligten technischen **Systeme und Dienste** (Hardware, Microservices, Software und Infrastruktur) ,
3. die technischen, organisatorischen und personellen **Prozesse** der Verarbeitung von Daten.

Der Ausdruck „Prozess“ ist in der DS-GVO nicht ausdrücklich enthalten. Jede Verarbeitungstätigkeit kann als Geschäftsprozess bzw. Fachverfahren modelliert werden; jede Verarbeitungstätigkeit besteht aus einzelnen Verarbeitungsschritten. Einzelne Verarbeitungen sind bspw. das Erheben, Erfassen, Ordnen oder Speichern bis zum Löschen oder Vernichten (vgl. Art. 4 Nr. 2 DS-GVO). Diese Verarbeitungen werden als Teilprozesse modelliert bzw. implementiert.

Methodisch stehen zunächst die Daten von Personen im Vordergrund, deren Erforderlichkeit der Verarbeitung an der Zweckbestimmung vorab zu bemessen ist.

Die konkrete funktionale Gestaltung geschieht auf der Ebene 1, auf der anhand der Daten der Schutzbedarf durch die verantwortliche Stelle festzustellen bzw. festzusetzen ist. Diesen Schutzbedarf erben alle Daten, Systeme und Prozesse, die bei einer konkreten Verarbeitung auf den verschiedenen Ebenen zum Einsatz kommen. Anhand des Referenzmaßnahmen- Katalogs kann überprüft werden, ob getroffene oder geplante technische und organisatorische Maßnahmen dem Schutzbedarf angemessen sind.

Bei diesen drei Kernkomponenten Daten, Systeme und Dienste sowie Prozesse spielen u. a. folgende spezielle Eigenschaften noch eine weitere zu beachtende Rolle:

Bei Daten sind Eigenschaften von **Datenformaten** zu betrachten, mit denen Daten erhoben und verarbeitet werden. Datenformate können Einfluss auf die Qualität der Umsetzung der Gewährleistungsziele haben, z. B. in den Fällen, in denen nicht als abschließend geklärt gelten darf, welche Inhalte Dateien mit bestimmten Formaten aufweisen. So können im Datenbestand von Textdateien vermeintlich gelöschte Daten enthalten sein, die im Ausdruck nicht erscheinen; Grafikdateien können Metadaten bspw. bzgl. Kameramodell, Ort und Zeit der Aufnahme enthalten oder es können wiederum relevante Informationen bei Grafik-, Video- und Audiodateien der Kompressionen zum Opfer fallen.

Bei den beteiligten Systemen sind die **Schnittstellen** zu betrachten, die eine Fachapplikation mit der Nutzung von IT-Systemen der Ebene 3 sowie insbesondere zu anderen Systemen, die nicht innerhalb der vom Zweck definierten Systemgrenze liegen, aufweist. Neben diesen vertikalen Schnittstellen sind auch horizontale Schnittstellen zu betrachten, mit denen ein Risiko für die Zweckbindung einhergeht. Der Ausweis der Existenz von Schnittstellen sowie die Dokumentation von deren Eigenschaften sind von entscheidender Bedeutung für die rechtliche Verantwortlichkeit, Beherrschbarkeit und Prüfbarkeit von Datenflüssen.

Für jede Verarbeitungstätigkeit und deren Komponenten, insbesondere für die manchmal schwierig fassbaren Prozesse über verschiedene Systeme hinweg gilt, die **Verantwortlichkeit** zu verdeutlichen und im Verzeichnis der Verarbeitungstätigkeiten in Art. 30 DS-GVO zu dokumentieren. Gemäß Art. 4 Abs. 7 ist ein Verantwortlicher „(…) eine natürliche oder juristische Person, Behörde oder Einrichtung (…), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet; (…).“ Aufgaben, die aus der Verantwortlichkeit resultieren, können in Form von individuellen Zuständigkeiten delegiert werden. Diese Zuständigkeiten werden typischerweise als Rollen in einem umfassenden Rollen- und Berechtigungskonzept formuliert und zugewiesen. Die Zuständigkeit eines Prozesseigentümers kann sich auf einzelne Verarbeitungen (Teilprozesse) oder auf die gesamte Verarbeitungstätigkeit über alle Prozessebenen hinweg im Sinne einer Gesamtzuständigkeit erstrecken. Diese Zuständigkeit kann auf unterschiedliche Rollen mit jeweils Teilzuständigkeiten verteilt werden. Wenn die Verarbeitungstätigkeit eine Auftragserarbeitung gemäß Art. 28 DS-GVO beinhaltet ist zu gewährleisten, dass der Auftragsverarbeiter seine Aufgaben gemäß den Weisungen des Verantwortlichen datenschutzkonform erfüllt.

Die Verantwortung für eine Verarbeitung liegt letztlich immer beim Verantwortlichen i. S. d. Art. 4 Abs. 7 DS-GVO.