Datenschutz Jahresbericht 2023

Prodware Deutschland AG

Am Sandtorkai 50

20457 Hamburg

PRW Consulting GmbH ● Leonrodstraße 54 ● D-80636 München ● Tel: +49 89 210977-70
Fax: +49 89 210977-77 ● info@prw-consulting.de ● www.prw-consulting.de
Geschäftsführer: Wilfried Reiners, Ralph Bösling
Steuernummer: 143/173/30201 – USt-IdNr.: DE247139957
HRB: 160557 – AG: München – FA: München für Körperschaften

Inhaltsverzeichnis

A. Allgemeiner Teil

1. Kontaktdaten

Auftraggeber als verantwortliche Stelle oder als Verantwortlicher

Name	Prodware Deutschland AG		
Straße / Ort	Am Sandtorkai 50 / 20457 Hamburg		
Telefon / Fax	+49 40 89958-0 / +49 40 89958-100		
Internet / E-Mail	www.prodwaregroup.com / info@prodware.de		
Ansprechpartner	**Funktion**	**Telefon**	**E-Mail**
Ian Mac Hueg Herlevsen	Vorstand	+49 40 89958-0	iherlevsen@prodware.de
Axel Pohl	Director Finance & Administration / Prokurist	+49 40 89958-384	a.pohl@prodware.de
Marc Launhardt	Lead Consultant	+49 40 89958-291	m.launhardt@prodware.de

Auftragnehmer des Mandats externer Datenschutzbeauftragter

Name	PRW Consulting GmbH		
Straße / Ort	Leonrodstraße 54 / 80636 München		
Telefon / Fax	+49 89 210977-70 / +49 89 210977-77		
Internet / E-Mail	www.prw-consulting.de / info@prw-consulting.de		
Ansprechpartner	**Funktion**	**Telefon**	**E-Mail**
Wilfried Reiners	Geschäftsführer	+49 89 210977-0	wilfried.reiners@prw-consulting.de
Ralph Bösling	Geschäftsführer	+49 89 210977-70	ralph.boesling@prw-consulting.de

Extern bestellter Datenschutzbeauftragter des Auftraggebers

Name	PRW Consulting GmbH		
Straße / Ort	Leonrodstraße 54 / 80636 München		
Telefon / Fax	+49 89 210977-70 / +49 89 210977-77		
Internet / E-Mail	www.prw-consulting.de / info@prw-consulting.de		
Ansprechpartner	**Funktion**	**Telefon**	**E-Mail**
Marcel Erntges	Datenschutzbeauftragter	+49 89 210977-70	marcel.erntges@prw-consulting.de

Zuständige Aufsichtsbehörde

Name	Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit		
Straße / Ort	Ludwig-Erhard-Str. 22 / 20459 Hamburg		
Telefon / Fax	+ 49 40 42854-4040 / +49 40 42854-4000		
Internet / E-Mail	www.datenschutz-hamburg.de / mailbox@datenschutz.hamburg.de		
Ansprechpartner	**Funktion**	**Telefon**	**E-Mail**
Thomas Fuchs	Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit	+ 49 40 42854-4040	mailbox@datenschutz.hamburg.de

2. Genereller Hinweis

Aus Gründen der besseren Lesbarkeit wird im Folgenden die Sprachform des generischen Maskulinums angewandt. Die juristische Fachsprache nutzt diese Form. Die ausschließliche Verwendung der männlichen Form wird geschlechtsunabhängig (m/w/d) verstanden.

3. Aufbau des Jahresberichtes

Dieser Jahresbericht gibt den Sachstand zum Datenschutz im angegebenen Berichtsjahr wieder. Der Berichtszeitraum richtet sich nach dem Geschäftsjahr des Auftraggebers. Der Bericht dient somit zum einen als Arbeitsnachweis, zum anderen werden künftig anstehende bzw. offene Arbeitsfelder beschrieben. Den Kapiteln ist vielfach eine kurze Beschreibung oder ein Verweis auf die Rechtsgrundlage vorangestellt. Dies soll zum besseren Verständnis dienen.
Hinweise zu den gesetzlichen Grundlagen werden z. B. in nachfolgender Form wiedergegeben:

Art. 1 Abs. 1 Satz 1 DSGVO: Gegenstand und Ziele

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Die Form der Berichtslegung durch den Datenschutzbeauftragten ist im Gesetz nicht geregelt. Allerdings ist mit der Umsetzungspflicht der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) eine deutliche Erweiterung der Dokumentations- und Rechenschaftspflichten einhergegangen. So hat der Verantwortliche nach Art. 5 Abs. 2 DSGVO die weitgehende Pflicht, die Einhaltung der in Art. 5 Abs. 1 DSGVO niedergelegten Grundsätze für eine ordnungsgemäße Datenverarbeitung nachzuweisen. Dazu gehören insbesondere die Grundsätze der Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Integrität und Vertraulichkeit. Der Datenschutzbeauftragte des Unternehmens sollte deshalb einmal im Jahr einen Tätigkeitsbericht erstellen. Dieser Datenschutzbericht dokumentiert alle vorgenommenen Maßnahmen hinsichtlich des Datenschutzes bei der Prodware Deutschland AG.

B. Besonderer Teil

I. Grundlagen

1. Genereller Rückblick auf 2023 und Ausblick auf 2024

a) NIS 2 Richtlinie - Handlungsbedarf

Die NIS-2-Richtlinie, auch bekannt als die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, wurde am 27.12.2022 im EU-Amtsblatt veröffentlicht und ist am 16.01.2023 in Kraft getreten, um die Cybersicherheit in der Europäischen Union zu stärken. Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese in nationales Recht überführen.

Sie dient als rechtlicher Rahmen für den Schutz von Netz- und Informationssystemen in kritischen Sektoren wie beispielsweise Energie, Gesundheitswesen und Finanzwesen. Sanktionen für Verstöße und eine verstärkte Rolle der nationalen Aufsichtsbehörden sind ebenfalls Teil dieser Regelungen. Ziel ist es, die Widerstandsfähigkeit der EU gegenüber Cyberbedrohungen zu stärken und gleichzeitig den freien Datenverkehr zu gewährleisten.

Die NIS-2-Richtlinie hat dabei Auswirkungen auch auf den Datenschutz, wenn es um die Sicherheit von Netz- und Informationssystemen geht. Die Richtlinie bezieht sich auf den Schutz kritischer Infrastrukturen und wesentlicher Dienste, zu denen auch Dienste im Bereich der elektronischen Kommunikation gehören. In diesem Zusammenhang gibt es Schnittstellen zu Datenschutzfragen.

Die NIS-2-Richtlinie und die Datenschutz-Grundverordnung (DSGVO) ergänzen sich in gewisser Weise. Beide Gesetze haben das gemeinsame Ziel, die Sicherheit personenbezogener Daten zu gewährleisten, wenn sie in Netz- und Informationssystemen verarbeitet werden. Die NIS-2-Richtlinie legt spezifische Anforderungen für Betreiber wesentlicher Dienste und digitaler Diensteanbieter fest, um die Sicherheit ihrer Systeme zu gewährleisten und sicherheitsrelevante Vorfälle zu melden. Diese Maßnahmen tragen indirekt zum Schutz personenbezogener Daten bei, da viele Dienste, die unter die NIS-Richtlinie fallen, auch personenbezogene Daten verarbeiten.

Es ist wichtig zu beachten, dass die DSGVO weiterhin die primäre Gesetzgebung im Bereich Datenschutz in der EU ist, aber die NIS-2-Richtlinie kann spezifische Anforderungen für den Schutz von Netz- und Informationssystemen und den Umgang mit Sicherheitsvorfällen festlegen, die sich auf personenbezogene Daten auswirken können.

b) EU-U.S. Data Privacy Framework

Am 10. Juli 2023 hat die Europäische Kommission einen Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework (deutsch: Datenschutzrahmen EU-USA, im Folgenden: Angemessenheitsbeschluss) erlassen. Damit attestiert sie den Vereinigten Staaten von Amerika (USA) ein angemessenes Schutzniveau für personenbezogene Daten, die innerhalb dieses Rahmens aus der Europäischen Union (EU) an US-Unternehmen als Datenimporteure übermittelt werden. Der Angemessenheitsbeschluss ist ein Durchführungsrechtsakt (Art. 291 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union - AEUV) in der Form eines an die Mitgliedstaaten gerichteten Beschlusses.

Der Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework bestätigt, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus der EU an die am EU-U.S. Data Privacy Framework teilnehmenden Unternehmen übermittelt werden.

Am EU-U.S. Data Privacy Framework nehmen US-Unternehmen teil, die hierfür zertifiziert sind und deshalb auf der "Data Privacy Framework List" stehen.

Der Angemessenheitsbeschluss vermittelt nicht allein eine Rechtsgrundlage für eine Drittlandübermittlung; Art. 5 ff. DSGVO sind kumulativ zu beachten.

Vom EU-U.S. Data Privacy Framework erfasst werden nahezu alle Übermittlungen personenbezogener Daten an US-Unternehmen, die sich im Rahmen eines Zertifizierungsmechanismus zur Einhaltung von bestimmten Datenschutzgrundsätzen verpflichtet haben. Voraussetzung für eine Zertifizierung ist, dass das betreffende US-Unternehmen der Aufsicht der U.S. Federal Trade Commission oder des U.S. Department of Transportation unterliegt; bei Unternehmen mit mehreren Sparten ist daher denkbar, dass nicht alle Unternehmensbereiche erfasst sind.

Auch die Übermittlung von Personaldaten ("HR Data"), die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, ist nicht automatisch vom EU-U.S. Data Privacy Framework erfasst, vielmehr muss das US-Unternehmen bei seiner Zertifizierung explizit angeben, dass sich diese auch auf die Übermittlung von Personaldaten beziehen soll. Damit geht insbesondere die Verpflichtung einher, mit den nationalen EU-Datenschutz-Aufsichtsbehörden zusammenzuarbeiten.

Die Datenexporteure müssen daher prüfen, ob ihre geplanten Datenübermittlungen in den Anwendungsbereich des Angemessenheitsbeschlusses fallen. Aus Gründen der Rechtssicherheit unterhält und pflegt das U.S. Department of Commerce eine Liste, die die US-Unternehmen enthält, die sich gemäß dem EU-U.S. Data Privacy Framework zertifiziert haben ("Data Privacy Framework List"). Dieser Liste kann auch entnommen werden, welche Gesellschaften einer Unternehmensgruppe zertifiziert sind ("covered entities") sowie welche Kategorien personenbezogener Daten ("covered

data") bzw. welche Wirtschaftszweige ("industries") umfasst werden. Die Liste sowie weitere Informationen von US-Seite zum EU-U.S. Data Privacy Framework stehen seit dem 17. Juli 2023 auf der Website https://www.dataprivacyframework.gov zur Verfügung.

Die Datenübermittlungen an US-Unternehmen, die nicht oder nicht für die gewünschte Übermittlung zertifiziert sind, müssen (weiterhin) auf eines der anderen in Art. 44 ff. DSGVO vorgesehenen Übermittlungsinstrumente gestützt werden.

Dabei gelten allerdings nach Mitteilung der EU-Kommission alle von der US-Regierung im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen unabhängig von den verwendeten Übermittlungsinstrumenten für alle Datenübermittlungen im Rahmen der Datenschutz-Grundverordnung an US-Unternehmen. Deshalb können Datenexporteure im Rahmen der Datenübermittlung mithilfe geeigneter Garantien (Art. 46 DSGVO) die von der EU-Kommission im Angemessenheitsbeschluss ausgeführten Bewertungen bei der Prüfung der Wirksamkeit des gewählten Übermittlungsinstruments ("Transfer Impact Assessment") berücksichtigen.

c) Künstliche Intelligenz aus Sicht der DSGVO

Keine andere Technologie wird derzeit mehr diskutiert in allen Wirtschaftszweigen, die so viele neue Möglichkeiten bietet, aber auch Ängste wecken kann. So können Prozesse durch Künstliche Intelligenz (KI) im Vertrieb, im Kundenservice, in der IT und bei vielen anderen Prozessen optimiert oder wirtschaftlicher gestaltet werden.

Neben den zahlreichen Vorteilen birgt der Einsatz von KI aber immer auch rechtliche Risiken für Unternehmen. Sollten im Bereich der Nutzung von KI auch personenbezogene Daten verarbeitet werden, sind alle Anforderungen der DSGVO durch das Unternehmen einzuhalten. Ist der Anwendungsbereich aktiviert, ist im Bereich der Künstlichen Intelligenz zum Beispiel eine Datenschutz-Folgenabschätzung gem. Art 35 DSGVO erforderlich und diese Risikoabschätzung ist bereits in der Planungsphase durchzuführen.

Zu den Grundsätzen der DSGVO gehören außerdem umfangreiche Dokumentationspflichten und um diese Dokumente datenschutzkonform zu erstellen, ist ein Verständnis der verwendeten KI und des Algorithmus für jedes Unternehmen eine Kernaufgabe. Die Gewichtungen der Kriterien, nach denen die KI lernt und entscheidet, müssen ebenso dokumentiert werden wie die Auswirkungen verschiedener Ergebnisse.

Wir unterstützen Sie gerne bei der Einführung und Nutzung von KI im Bereich Datenschutz mit unserem Know-how im Bereich dieser neuen Technologie.

d) EUGH-Urteile mit Datenschutzrelevanz

Bußgelder zum Datenschutz erreichten im Jahr 2023 ein neues Rekordhoch. Europäische und deutsche Gerichte stärken mit ihren aktuellen Urteilen den Schutz personenbezogener Daten und geben Rechtssicherheit für Unternehmen hinsichtlich des Umgangs mit personenbezogenen Daten. Folgende Entscheidungen sind besonders relevant:

Zulässige Speicherdauer einer Videoüberwachung

Personenbezogene Daten dürfen nicht länger gespeichert werden, als es für die Zwecke, für die sie verarbeitet wurden, erforderlich ist. Im vorliegenden Fall ging es um eine Selbstbedienungstankstelle, die Videoaufzeichnungen wurden zur Aufklärung von Straftaten vorgenommen und dementsprechend gespeichert. Das Gericht entschied, dass zu diesem Zweck eine Zeitspanne von 72 Stunden ausreiche – danach müssen die Aufzeichnungen gelöscht werden. Längere Speicherfristen sind zu begründen (VG Hannover (10. Kammer), Urteil vom 13.03.2023 – 10 A 1443/19).

Kein Anspruch einer juristischen Person aus der DSGVO

Juristischen Personen bleibt die Geltendmachung von Ansprüchen auf Unterlassung oder Beseitigung gegenüber Dritten auf Grundlage der DSGVO verwehrt. Die DSGVO dient dem Schutz personenbezogener Daten, also von Informationen, die sich auf eine identifizierte oder identifizierbare natürliche und betroffene Person beziehen. Damit schützt sie nur die personenbezogenen Daten der Beschäftigten der juristischen Person, nicht aber die juristische Person selbst (OLG Dresden (4. Zivilsenat), Urteil vom 14.03.2023 – 4 U 1377/22).

Weigerungsrecht bei missbräuchlichen Auskunftsanträgen

Ein Anspruch auf Auskunftserteilung (Artikel 15 DSGVO) besteht nur dann, wenn hiermit auch legitime Zwecke verfolgt werden, also keine rechtsmissbräuchlichen oder exzessiven Auskunftsersuche vorliegen. Letzteres wurde für ein Auskunftsersuchen entschieden, das als datenschutzrechtliches Ersuchen getarnt war, aber eigentlich den Zweck verfolgte, die von der privaten Krankenversicherung vorgenommenen Prämienerhöhungen auf Mängel hin zu überprüfen. In einem weiteren Verfahren war die Überprüfung arzthaftungsrechtlicher Ansprüche der Hintergrund eines Auskunftsantrags. Das Auskunftsersuchen stelle kein „Allzweckwerkzeug“ für alle Auskünfte dar und kann nicht genutzt werden, um beispielsweise Informationen für zivilrechtliche Verfahren zu erlangen. Dies wäre missbräuchlich und berechtigt daher Unternehmen, in solchen Fällen die Auskunft zu verweigern, ohne Bußgelder und Schadensersatzansprüche zu riskieren (OLG Brandenburg (11. Zivilsenat), Urteil vom 14.04.2023 – 11 U 233/22 und BGH, Beschluss vom 29.3.2022 – VI ZR 1352/20).

Schmerzensgeld bei Datenschutzverstößen

Das Arbeitsgericht Oldenburg hat einem ehemaligen Arbeitnehmer einen Schmerzensgeldanspruch in Höhe von 10.000 Euro zugesprochen. Das Unternehmen war dem Auskunftsanspruch des Klägers nach Artikel 15 DSGVO nicht nachgekommen. Ein solcher Schmerzensgeldanspruch besteht parallel zu einem potenziellen Bußgeld durch die zuständige Aufsichtsbehörde (ArbG Oldenburg, Urteil vom 9.2.2023 – 3 Ca 150/21).

Der europäische Gerichtshof (EuGH) stellt allerdings klar, dass ein Datenschutzverstoß nicht zwangsweise einen Schmerzensgeldanspruch rechtfertigt. Es muss zusätzlich ein durch den Verstoß verursachter materieller oder immaterieller Schaden vorliegen. Dieser Schaden muss zwar nicht die Schwelle sogenannter Bagatellschäden überschreiten, es muss aber mehr als das „subjektive Unmutsgefühl" beeinträchtigt sein. Der Schadensersatzanspruch soll auch einen abschreckenden Effekt haben: Die Wiederholung rechtswidriger Verhaltensweisen soll verhindert werden (EuGH, 04.05.2023 – C-300/21).

Löschung von Google-Suchergebnissen

Wer erreichen möchte, dass einzelne Ergebnisse der Google-Suche über seine Person gelöscht werden, muss „relevante und hinreichende Nachweise" dafür vorlegen, dass die Suchergebnisse offensichtlich unrichtige Informationen enthalten. Suchmaschinenbetreiber sind nicht dazu verpflichtet, bzgl. der Richtigkeit der Informationen selbst zu ermitteln und Links zu Artikeln mit potenziell falschen Angaben zu entfernen. Im konkreten Fall ging es um Personen aus der Finanzdienstleistungsbranche, die sich durch mehrere kritische Artikel über ihr Anlagemodell verleumdet sahen. Diese Artikel waren von amerikanischen Internetseiten veröffentlicht worden. Google entfernte die Artikel nicht, mit der Begründung, man könne den Wahrheitsgehalt schlichtweg nicht beurteilen. Zu Recht, so der BGH, denn das Klägerpaar konnte die offensichtliche Unwahrheit nicht nachweisen. Was allerdings nicht in der Trefferliste angezeigt werden darf, sind Fotos ohne jeglichen Kontext (sog. Thumbnails). Das gilt auch dann, wenn man mit einem Klick auf die Artikelseite gelangt. Hier überwiegt das Recht am eigenen Bild (BGH, Urteil vom 23.05.2023 - VI ZR 476/18).

2. Datenschutzmanagement

Die DSGVO verpflichtet die verantwortliche Stelle implizit, ein Datenschutzmanagement einzuführen, das den Schutz der personenbezogenen Daten sicherstellen soll. Wer den Datenschutz ernsthaft umsetzen und implementieren möchte, kann auf ein solches System nicht verzichten, weil das „Handling" des modernen Datenschutzes in einer Vielzahl von Vorschriften geregelt ist und strukturiert werden muss, z. B.:

- Art. 5 DSGVO stellt die Grundsätze für die Verarbeitung personenbezogener Daten dar;
- Art. 30 DSGVO legt dem Verantwortlichen auf, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen;
- Art. 32 DSGVO regelt, dass der Verantwortliche und der Auftragsverarbeiter geeignete **T**echnische und **O**rganisatorische **M**aßnahmen (TOM) umzusetzen zu haben, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung von personenbezogenen Daten gemäß der DSGVO erfolgt;
- Art. 35 DSGVO verpflichtet den Verantwortlichen bei Verarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchzuführen.

Die PRW Consulting GmbH („PRW") hat, gemeinsam mit dem Auftraggeber, Prodware Deutschland AG, ein solches System eingeführt. Es finden regelmäßige Jour Fixe Termine statt, um die Anforderungen des Datenschutzmanagement-Systems zu erfüllen.

Dieser Bericht zeigt auf, wie die verantwortliche Stelle, gemeinsam mit dem Datenschutzbeauftragten, die Datenschutzanforderungen im Jahr 2023 gemanagt haben.

3. Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO)

Art. 37 Abs. 1 lit. b) DSGVO: Benennung eines Datenschutzbeauftragten

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und / oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Die Benennung des Datenschutzbeauftragten erfolgte ordnungsgemäß und ist an die in den Kontaktdaten aufgeführte Aufsichtsbehörde übermittelt worden. Den Beschäftigten der Prodware Deutschland AG ist der Datenschutzbeauftragte vorgestellt worden und bekannt.

4. Einbindung des Datenschutzbeauftragten (Art. 39 DSGVO)

Art. 39 DSGVO: Aufgaben des Datenschutzbeauftragten

Abs. 1 Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

lit. a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

lit. b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

lit. c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

lit. d) Zusammenarbeit mit der Aufsichtsbehörde;

lit. e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Abs. 2 Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Der Datenschutzbeauftragte wurde in alle relevanten Datenschutzthemen im Jahr 2023 eingebunden.

Der Datenschutzbeauftragte wird im folgenden Jahr 2024 regelmäßig Abfragen durchführen, um eventuell neue oder geänderte Verfahren der Verarbeitung personenbezogener Daten frühzeitig zu identifizieren.

II. Dokumentation des Datenschutzes im Jahr 2023

1. Jahresgespräch (Art. 39 Abs. 1 lit. a) DSGVO)

Art. 39 DSGVO: Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

Der Datenschutzbeauftragte hat am 28.05.2024 ein Jahresgespräch vor Ort bei der Prodware Deutschland AG, mit diversen Ansprechpartnern durchgeführt. Entsprechende Ergebnisse sind im Protokoll des Jahresgesprächs niedergelegt.

2. Informationspflichten / Betroffenenrechte (Art. 12 ff. DSGVO)

Art. 12 DSGVO: Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person.

Art. 13 DSGVO: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person.

Art. 14 DSGVO: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

Die DSGVO sieht eine Vielzahl von Informationspflichten vor. Das Gesetz unterscheidet neben dem Transparenzgebot zwischen zwei (2) Fällen der Informationspflicht: Zum einen, wenn die personenbezogenen Daten bei dem Betroffenen direkt erfasst werden (Art. 13 DSGVO) und zum anderen, wenn diese nicht bei der betroffenen Person erhoben werden (Art. 14 DSGVO).

Werden die Daten zur Kommunikation mit der betroffenen Person verwendet, besteht die Informationspflicht direkt bei Kontaktaufnahme.

Erfolgt die Erhebung nicht beim Betroffenen, ist dieser innerhalb einer angemessenen Frist, spätestens aber nach einem (1) Monat, zu informieren.

Inhaltlich treffen den Verantwortlichen auch bei dieser Art der Erhebung grundsätzlich die gleichen Informationspflichten. Eine Ausnahme bildet dabei nur die Information über die Verpflichtung zur Bereitstellung, da der Verantwortliche nicht selbst über diese entscheiden kann. Zusätzlich trifft ihn die Pflicht, darüber zu informieren, aus welcher Quelle die Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Den Informationspflichten ist in präziser, transparenter, verständlicher und leicht zugänglicher Form nachzukommen. Dabei können diese schriftlich oder in elektronischer Form an den Betroffenen übermittelt werden. Es wird explizit erwähnt, dass dafür auch sog. standardisierte Bildsymbole verwendet werden können, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

Der Gesetzgeber hat den Informationspflichten somit einen hohen Stellenwert eingeräumt. Die meisten **Bußgelder** beruhen auf **fehlenden Informationspflichten** und **fehlenden Löschkonzepten**.

Die Dokumente zu den Informationspflichten wurden erstellt. Alle Informationspflichten enthalten die notwendigen DSGVO-Anforderungen und sind leicht verständlich sowie jederzeit für die Betroffenen ersichtlich.

3. Vertraulichkeitsvereinbarung / Richtlinie

Art. 28 Abs. 3 lit. b) DSGVO: Auftragsverarbeiter

Gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Die Vertraulichkeitsvereinbarung für die eigenen Mitarbeiter ist ausgerollt und entspricht den Anforderungen der DSGVO. Außerdem wurde im Bereich der Richtlinien eine (1) Datenschutzrichtlinie erstellt und verabschiedet.

4. Löschkonzept - LK - (Art. 17 DSGVO)

Art. 5 Abs. 1 lit. e) DSGVO: Grundsätze für die Verarbeitung personenbezogene Daten

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung").

Art. 17 Abs. 1 lit. a) DSGVO: Recht auf Löschung

Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

Aufgrund konkretisierter Best-Practice-Ansätze und Abfragen nach dem Vorhandensein eines Löschkonzepts seitens der Aufsichtsbehörden ist die Erstellung eines detaillierten Löschkonzepts dringend zu empfehlen, in welchem neben den entsprechenden Fristen auch die Maßnahmen dokumentiert sind, wie die Frist eingehalten und die Löschung durchgeführt wird. In der ersten Projektphase eines Löschkonzepts sollte der Katalog der Löschregeln möglichst vollständig erstellt werden. Dazu sind erfahrungsgemäß mehrere Abstimmungsrunden mit Fachverantwortlichen, Juristen, Technikern und Datenschützern notwendig.

Die Löschfristen für die einzelnen Verarbeitungen wurden im Verarbeitungsverzeichnis (VVZ) dokumentiert.

5. Auftragsverarbeitung (Art. 28 DSGVO)

Art. 28 Abs. 3 Satz 1 DSGVO: Auftragsverarbeiter

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Alle AVV-Muster liegen vor. Kunden erhalten bei der Beauftragung einen AVV, wenn dies notwendig ist. Die DSGVO erfordert, dass die Auftragsverarbeiter-Liste komplett und aktuell ist. Dem DSB liegt eine aktuelle AVV-Liste vor.

6. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 und Abs. 2 DSGVO)

a) Verarbeitungsverzeichnis (VVZ) nach Art. 30 Abs. 1 DSGVO

Art. 30 Abs. 1 Satz 1 DSGVO: Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.

Die VVZ wurden identifiziert und erstellt, sowie im Jahr 2023 aktualisiert.

b) Verarbeitungsverzeichnis (VVZ) nach Art. 30 Abs. 2 DSGVO

Art. 30 Abs. 2 Satz 1 DSGVO: Verzeichnis von Verarbeitungstätigkeiten

Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

Die Regelung in Art. 30 DSGVO verpflichtet auch Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO Verzeichnisse von Verarbeitungstätigkeiten, die sie im Auftrag durchführen, zu erstellen und zu führen. Die Regelung des Art. 30 DSGVO bezieht auch den Vertreter im Sinne von Art. 4 Nr. 17 DSGVO mit ein.

Neben der Umsetzung der Verpflichtung nach Art. 30 DSGVO kann das Verzeichnis als Grundlage zur Erfüllung weiterer datenschutzrechtlicher Pflichten verwendet werden.

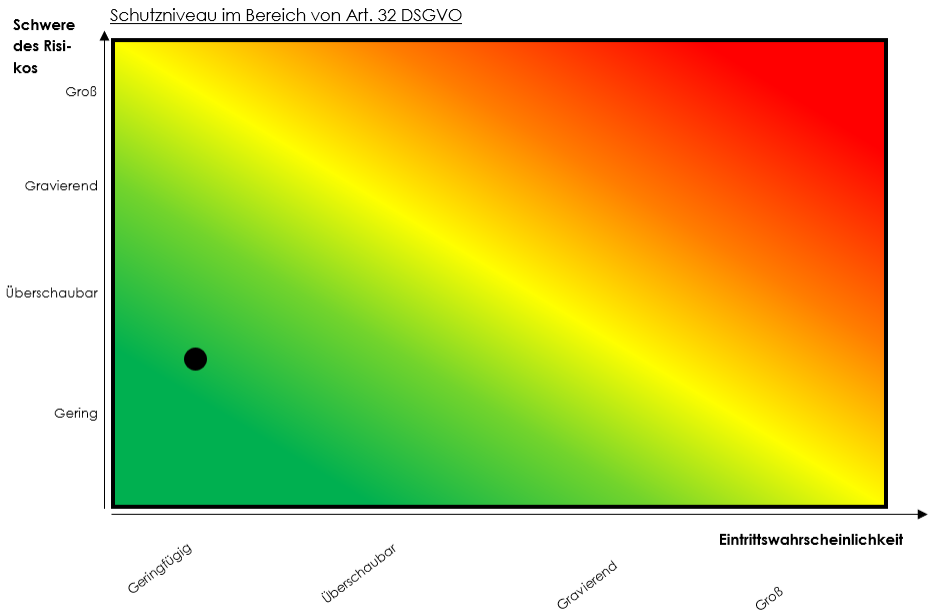
7. Technische und Organisatorische Maßnahmen – TOM – (Art. 32 DSGVO)

Art. 32 Abs. 1 DSGVO: Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

§ 64 BDSG Anforderungen an die Sicherheit der Datenverarbeitung.

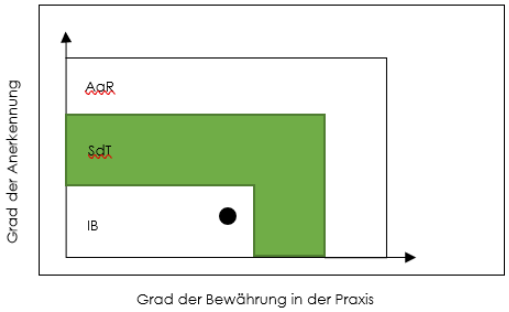
Grundsätzlich steht es jedem Verantwortlichen frei, selbst diejenigen TOM auszuwählen, die passend zu der eigenen Art der Verarbeitung und Unternehmensgröße sind, sofern damit ein wirksames angemessenes Schutzniveau erreicht werden kann. Die DSGVO, als auch die Aufsichtsbehörden, fordern jedoch verstärkt die Einhaltung oder mindestens die Berücksichtigung des „Stands der Technik" der TOM. Eine weitere Konkretisierung der relevanten Systeme und Komponenten erfolgt seitens des Gesetzgebers nicht. Daher müssen die entsprechenden Sicherheitsmaßnahmen regelmäßig einer Bewertung unterzogen werden, ob weiterhin unter Berücksichtigung des Stands der Technik ein angemessenes Schutzniveau gewährleistet wird.
Ausgangspunkt bei der Bewertung der erforderlichen TOM muss immer eine Risikoanalyse bzw. die Betrachtung des erforderlichen Schutzniveaus sein (siehe **Bild 1**) sowie die Betrachtung des Stands der Technik im Bereich der implementierten Maßnahmen (siehe **Bild 2**).



(Bild 1 Bewertung des Schutzniveaus)

Bestimmung des Technologiestandes ☐ Stand der Technik (SdT) ☒ Interne Bewertung (IB) ☐ Allg. anerkannte Regeln (AaR)

Einordnung des Technologiestandes



(Bild 2 Bestimmung des Technologiestands)

Die TOM wurden erstellt und sind gesondert abgelegt. Die derzeit dokumentierten und implementierten TOM erfüllen im Bereich der Sicherheit der entsprechenden personenbezogenen Daten die Anforderungen des Art. 32 DSGVO.

8. Datenschutzverletzung (Art. 33 DSGVO)

Art. 33 Abs. 1 DSGVO: Meldung von Verletzungen des Schutzes personenbezogener Daten betroffenen Person

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Neben der gesetzlichen Regelung wurde mit dem Auftraggeber die Frage geklärt, wann es sich um einen Vorgang der Verletzung des Schutzes personenbezogener Daten handelt. So wurde ein einheitliches Verständnis geschaffen, das sich wie folgt zusammenfassen lässt: Datenschutzvorfälle sind Unregelmäßigkeiten in der Verarbeitung von personenbezogenen Daten, die zu einem Risiko für die Betroffenen führen. Wichtig war dabei die Festlegung, dass bei der Definition des Datenschutzvorfalls noch keine Bewertung der Meldeverpflichtung gegenüber Behörden oder Betroffenen vorgenommen wird, da auch nicht meldepflichtige Verstöße für die Bewertung des Datenschutzniveaus essenziell sind.

- Im Jahr 2023 erfolgte eine Sensibilisierung der Mitarbeiter in den Datenschutzschulungen zum Verhalten bei einer vermeintlichen Datenschutzverletzung.
- Für die Prodware Deutschland AG wurde ein Musterdokument erstellt, welches die notwendigen Informations- und Eskalationsprozesse ausführlich darstellt.
- Mit den Verantwortlichen wurden die notwendigen Vorgehensweisen innerhalb von Schulungs- und Sensibilisierungsmaßnahmen besprochen.

9. Datenschutz-Folgenabschätzung - DSFA - (Art. 35 DSGVO)

Art. 35 Abs. 1 und 2 DSGVO: Datenschutz-Folgenabschätzung

Abs. 1 Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Abs. 2 Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

Im Bereich der DSFA haben sich wesentliche Änderungen seitens der Behörden ergeben. Die Datenschutzkonferenz (DSK), Versammlung der Landesdatenschutzbehörden, hat ein Muster verabschiedet, indem die Dokumentation einem völlig überarbeiteten Risiko-Analyse basierten Ansatz folgt. Die Beschreibung der Verarbeitung und die Darstellung der Risikooptionen ist wesentlich dedizierter durchzuführen.
Die nachfolgende detaillierte Erläuterung der deutschen Aufsichtsbehörden (gemäß Art. 35 DSGVO; § 67 BDSG) wurde mit dem Auftraggeber besprochen. Folgende Verarbeitungstätigkeiten unterliegen der Pflicht einer vorherigen DSFA.

1. Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung von Personen, soweit diese Verarbeitung (die Erfüllung eines der folgenden Merkmale genügt):

- besonders schutzwürdige Personen betrifft;
- der systematischen Überwachung dient;
- unter innovativer Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen erfolgt;
- der Bewertung oder Einstufung (Scoring) dient;
- bei gleichzeitiger Abgleichung oder Zusammenführung von Datensätzen erfolgt;

- im Rahmen einer automatisierten Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung erfolgt;
- Betroffene an der Ausübung ihrer Rechte, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags hindert.

2. Verarbeitung von genetischen Daten, soweit diese Verarbeitung (die Erfüllung eines der folgenden Merkmale genügt):
- besonders schutzwürdige Personen betrifft;
- der systematischen Überwachung dient;
- unter innovativer Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen erfolgt;
- der Bewertung oder Einstufung (Scoring) dient;
- bei gleichzeitiger Abgleichung oder Zusammenführung von Datensätzen erfolgt;
- im Rahmen einer automatisierten Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung erfolgt;
- Betroffene an der Ausübung ihrer Rechte, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags hindert.

3. Umfangreiche Verarbeitung von Daten, die einem Sozial-, Berufs- oder Amtsgeheimnis unterliegen.

4. Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von Menschen.

5. Optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, die in großem Umfang zentral zusammengeführt werden.

6. Umfangreiche Erhebung, Veröffentlichung oder Übermittlung von personenbezogenen Daten zur Bewertung von Verhalten oder anderer persönlicher Aspekte von Menschen, soweit diese von Dritten dazu genutzt werden können, Rechtswirkung gegenüber der bewerteten Person zu entfalten oder diese in ähnlich erheblicher Weise zu beeinträchtigen.

7. Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung der Arbeitstätigkeit eingesetzt werden können, sodass sich Rechtsfolgen für den Betroffenen ergeben oder ihn in anderer erheblicher Weise beeinträchtigen.

8. Erstellung umfassender Profile über Interessen, das Netz ihrer persönlichen Beziehungen, sowie die Persönlichkeit von Menschen.

9. Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung dieser Daten, sofern dies in großem Umfang erfolgt oder für Zwecke, für die nicht alle Daten bei der betroffenen Person direkt erhoben wurden, oder wenn dies unter Einsatz von Algorithmen geschieht, die für die betroffenen Personen nicht nachvollziehbar sind, oder die Verarbeitung erfolgt, um bislang unbekannte Zusammenhänge zwischen den Daten zu bislang nicht festgelegten Zwecken zu entdecken (Datamining).
10. Verarbeitung unter Einsatz von künstlicher Intelligenz zur Steuerung einer Interaktion mit dem Betroffenen oder zur Bewertung persönlicher Aspekte.

11. Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts oder von Funksignalen, die von solchen Geräten versendet werden, zur Ermittlung von Aufenthaltsorten oder Bewegungen von Personen über einen substanziellen Zeitraum.

12. Automatisierte Auswertung von Video- oder Audioaufnahmen zur Bewertung von Persönlichkeiten.

13. Erstellung umfassender Profile über Bewegung und Kaufverhalten von Personen.

14. Anonymisierung besonderer personenbezogener Daten zum Zwecke der Übermittlung an Dritte, soweit dies in Bezug auf die Zahl der betroffenen Personen als auch den Angaben je Person nicht nur in Einzelfällen erfolgt.

15. Die auch nicht umfangreiche Verarbeitung von besonderen personenbezogenen Daten sowie von Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten unter Verwendung neuer Technologien zur Bestimmung der Leistungsfähigkeit von Personen.

Alle durchgeführten DSFA wurden zur Dokumentation gesondert abgelegt und im Jahr 2023 aktualisiert.

10. Schulungs- / Sensibilisierungsmaßnahmen (Art. 39 DSGVO)

Art. 39 Abs. 1 lit. b) DSGVO: Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.

Ein Schulungsprogramm wurde eingeführt. Jeder Mitarbeiter muss die Schulung durchführen und eine entsprechende Prüfung abschließen.

Eine Auffrischungsschulung mit aktuellen Themen zur Entwicklung der Rechtsprechung innerhalb der DSGVO und den daraus erforderlichen Handlungsempfehlungen wird im Jahr 2024 durchgeführt werden.

11. Anfragen intern / extern (Art. 39 DSGVO)

Art. 39 Abs. 1 lit. a) DSGVO: Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten.

Für interne und externe Fragen zum Thema Datenschutz steht der Datenschutzbeauftragte sowohl Mitarbeitern als auch extern betroffenen Personen zur Verfügung. Dies ist beim Auftraggeber bekannt und gilt selbstverständlich für das kommende Berichtsjahr fort.

Im Jahr 2023 fanden zahlreiche Telefonate mit dem Datenschutzbeauftragten statt und es wurden zahlreiche Anfragen bearbeitet.

12. Drittstaatenproblematik (Art. 44 ff. DSGVO)

Art. 44 – 50 DSGVO: Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen.

Die DSGVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union (EU) / des Europäischen Wirtschaftsraums (EWR) besondere Regelungen vor (Art. 44 - 49 DSGVO). Länder außerhalb der EU / des EWR werden in der DSGVO als „Dritt-länder" bezeichnet. In der Praxis wird auch der Begriff „Drittstaat" verwendet.

Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob - unabhängig von den in den Art. 45 ff. DSGVO geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer - auch alle übrigen Anforderungen der DSGVO (z. B. Art. 9 Abs. 3) an die in Rede stehende Datenverarbeitung eingehalten werden **(1. Stufe).** Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Art. 44 DSGVO zusätzlich die spezifischen Anforderungen der Art. 45 ff. DSGVO an die Übermittlung in Drittländer beachtet werden **(2. Stufe).** Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 Satz 1 2. HS DSGVO).

- Im Jahr 2023 erfolgte eine Überprüfung der Drittlandthematik. Diese stellt sich abschließend für die Prodware Deutschland AG im Bereich des Dienstleisters **Microsoft** als relevant dar.
- **Die Drittlandthematik wurde angesprochen**. Zurzeit werden im Microsoft Umfeld die neuen EU-Standardvertragsklauseln für die Übermittlung in Drittländer verwendet.

Nachfolgende Schritte bei der Übermittlung von personenbezogenen Daten in ein Drittland sind einzuhalten:

- Schritt 1: Datenübermittlung kennen;
- Schritt 2: Auswahl der eingesetzten Übermittlungsinstrumente;
- Schritt 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Art. 46 DSGVO;
- Schritt 4: ggf. zusätzliche Maßnahmen ergreifen;
- Schritt 5: Verfahrensschritte nach Ermittlung effektiver zusätzlicher Maßnahmen;
- Schritt 6: Neubewertung Datenübermittlung durch den Datenexporteur in angemessenen Abständen.

Des Weiteren empfiehlt der Europäische Datenschutzausschuss (EDSA) dem Datenexporteur als Verantwortlichen eine DSFA durchzuführen. Durch eine DSFA können abstrakte Gefahren durch Rechtslagen im Zielland (z. B. rechtswidrige Zugriffe durch Behörden) analysiert werden und ggfs. zusätzliche Maßnahmen implementiert werden.

Die Prodware Deutschland AG hat diese Maßnahmen umgesetzt.

13. Fazit zu 2023

Die Anforderungen der DSGVO und des BDSG sind bei der Prodware Deutschland AG sehr gut umgesetzt. Dies ist in diesem Bericht dokumentiert. Die wesentlichen Elemente des Datenschutzes (Grundsätze der Verarbeitung personenbezogener Daten und Rechtmäßigkeit der Verarbeitung) werden durchgängig beachtet. Der Datenschutzbeauftragte Herr Marcel Erntges / PRW bedankt sich für die professionelle Unterstützung und ausgezeichnete Zusammenarbeit mit der Prodware Deutschland AG. In den Gesprächen mit den Mitarbeitern ist für den Datenschutzbeauftragten erkennbar, dass diese sehr gut auf die Relevanz und Notwendigkeit von Datenschutzkonformität sensibilisiert sind.

C. Ausblick auf 2024

1. Zusammenarbeit

Die im Rubrum aufgeführten Parteien haben die weitere Zusammenarbeit, auch für den Berichtszeitraum 2024, beschlossen.

München, den 24.06.2024

Marcel Erntges
PRW Consulting GmbH