Datenschutz Jahresbericht 2022

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. Der Bericht erläutert außerdem bereits erfolgte und geplante Anpassungen von Aktivitäten und Dokumentationen im Datenschutz. Er endet mit Empfehlungen und Optionen für 2023.

B. Besonderer Teil

I. Grundlagen

1. Genereller Rückblick auf 2022

a) Corona Pandemie

Mit der am 19.11.2021 im Infektionsschutzgesetz beschlossenen 3G-Regel am Arbeitsplatz wurden hiernach nun alle Unternehmen mit Sitz in Deutschland verpflichtet, von ihren Mitarbeitern mit Personenkontakt im Unternehmen einen Nachweis über die Impfung, Genesung oder eines max. 24 Stunden alten negativen (Antigen-Schnell-) Tests zu verlangen.

Mit Ablauf der Regelung am 19.03.2022 müssen nun alle erfassten personenbezogenen Daten der Mitarbeiter und Besucher gelöscht werden.

b) Datentransfer-Folgenabschätzung (TIA)

Im Zuge der neuen Standardvertragsklauseln hat die sog. Datentransfer-Folgenabschätzung (TIA) dieses Jahr hohe Wellen geschlagen. Sie ist verpflichtend dokumentiert durchzuführen, bevor man die neuen Standardvertragsklauseln abschließt. Zum Inhalt dieser Abschätzung besagt Klausel 14 der neuen Standardvertragsklauseln:

„*Der Verantwortliche muss versichern können, dass der Vertragspartner aus dem Drittland in der Lage ist, seinen Pflichten aus den Standardvertragsklauseln nachzukommen. Hierzu gehört, dass die Datenübermittlung mit Art der Daten, Zweck der Datenverarbeitung, Kategorien der Betroffenen, Art des Empfängers, Verarbeitungsketten sowie das Empfängerland mit dessen Rechtsvorschriften und Gepflogenheiten in Bezug auf Datenzugriffe genau beschrieben werden.*“

Schließlich sollte die TIA beschreiben, welche zusätzlichen Garantien und Maßnahmen für eine sichere Datenverarbeitung gewählt wurden. Fällt die Abwägung negativ aus, sollten keine Daten an den Vertragspartner im Drittland übermittelt werden.

c) Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)

Ein weiterer datenschutzrechtlicher Meilenstein war das am 01.12.2021 in Deutschland in Kraft getretene Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) als nationale Umsetzung der seit längerem bekannten ePrivacy-Richtlinie. Dieses dient u. a. dem Schutz von personenbezogenen Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien und setzt insbesondere die Anforderungen aus dem Planet49-Urteil in nationales Recht um.

Die DSGVO gilt natürlich weiter und ist grundsätzlich vorrangig gegenüber nationalen Datenschutzbestimmungen zu beachten. In Bezug auf den „Schutz der Privatsphäre bei Endeinrichtungen“ gelten DSGVO und TTDSG nebeneinander.

Hier ist - insbesondere neben der DSGVO - § 25 TTDSG zu beachten, der im Speziellen für Websitebetreiber und sonstige Anbieter von Telemedien relevant ist. Hiernach bedarf die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, einer Einwilligung des Endnutzers.

Diese Regelung gilt sowohl für personenbezogene als auch nicht personenbezogene Daten, sie ist technologieneutral gefasst und betrifft neben dem Einsatz von Cookies auch sonstige Techniken, die ein Speichern und / oder Auslesen von Informationen auf Endeinrichtungen erfordern. Die Einwilligung, die sich nach den DSGVO-Vorschriften richtet, kann, wie auch bei Cookies, über den Cookie-Banner eingeholt werden.

d) EU-Standardvertragsklauseln (SCC)

Am 04. Juni 2021 hat die EU-Kommission die neuen EU-Standardvertragsklauseln SCC (Standard Contractual Clauses) veröffentlicht. Mit den neuen Standardvertragsklauseln soll die Übermittlung für Datenübertragungen aus der EU in Drittländer (Nicht-EU-Länder) erleichtert werden.

Die neuen SCC sehen verschiedene Datenübermittlungsvarianten vor:

- Modul EINS betrifft die Übermittlung von personenbezogenen Daten zwischen zwei (2) Verantwortlichen.
- Modul ZWEI betrifft die Datenübermittlung vom Verantwortlichen an den Auftragsverarbeiter.
- Modul DREI betrifft die Datenübermittlung zwischen zwei (2) Auftragsverarbeitern.
- Modul VIER betrifft den Datentransfer von Auftragsverarbeitern an Verantwortliche.

Die modernisierten SCC ersetzen die unter der vorherigen Datenschutzrichtlinie 95/46 verabschiedeten SCC. Sie sind die konsequente Weiterentwicklung der Anforderungen des EuGHs (Gerichtshof der Europäischen Union) aus der sog. Schrems II Entscheidung.

Verantwortliche und Auftragsverarbeiter sind aufgefordert, ihre bestehenden Verträge und Vertragsverhältnisse zu überprüfen und ggf. die neuen SCC mit den Vertragspartnern zu vereinbaren. Weiter bestehen bleibt die Einzelfallprüfung, da laut EuGH ggfs. zusätzliche Schutzmaßnahmen implementiert werden müssen.

Die überarbeiteten SCC schreiben erstmals Garantien vor, „um etwaige Auswirkungen der Gesetze des Bestimmungsdrittlands" auf die Einhaltbarkeit der Klauseln durch den Datenimporteur zu regeln.

Dabei gilt es vor allem darum, vorab zu klären, „wie mit verbindlichen Ersuchen von Behörden im Drittland nach einer Weitergabe der übermittelten personenbezogenen Daten umzugehen ist". Getragen werden die Regeln von dem Verständnis, dass Gesetze, die das Wesen der Grundrechte und -freiheiten respektieren und in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, beachtet werden.

Die datenexportierenden Unternehmen kommen somit auf Grundlage der neuen SCC nicht umhin, zu prüfen, ob nationales Recht im Drittland zu einer Verletzung der Rechte und Freiheiten von Betroffenen führt und somit zusätzliche Maßnahmen für den Schutz der personenbezogenen Daten notwendig sind. Hierzu ist zu empfehlen, die konkreten Datentransfers zu analysieren und festzustellen, welche Gesetze des Drittlandes jeweils Anwendung finden. Für das Gros der Industrieländer sind diese Regelungen bekannt. Im Einzelfall kann es möglich sein, dass Recherchen angestellt werden müssen. Hierbei unterstützen uns unsere Kollegen bei PRW Rechtsanwälte.
Für Verantwortliche und Auftragsverarbeiter, die aktuell die bisher bestehenden SCC für Übermittlungen in Drittländer verwenden, sieht der Beschluss zu den neuen SCC eine Übergangsfrist von achtzehn (18) Monaten vor. Die Übergangsfrist läuft am 27. Dezember 2022 ab.

e) EU Data Act

Die EU-Kommission hat am 23. Februar 2022 ihren Entwurf einer neuen Verordnung zur Regelung des fairen Zugangs zu und der Nutzung von Daten („Data Act“) vorgestellt. Ziel ist es, durch neue Regelungen das wirtschaftliche Potential der immer größer werdenden Datenmenge besser zu nutzen.

In sieben (7) Kapiteln enthält der Entwurf des Data Acts unter anderem Regelungen zum Datenaustausch zwischen den Akteuren, zur Bereitstellung von Daten, zu unfairen Vertragsklauseln sowie zur Interoperabilität und zum Wechsel von Datenverarbeitungsdiensten.

Dem Entwurf des Data Acts liegt ein sehr weiter Begriff von Daten zugrunde. Es werden jegliche digitalen Darstellungen von Handlungen, Tatsachen oder Informationen sowie jede Vermengung dieser Handlungen, Tatsachen oder Informationen, auch in Form von Ton, Bild oder audiovisuellen Aufzeichnungen, erfasst.

Die Regelungen des Entwurfs des Data Acts sollen sowohl auf die Hersteller von vernetzten und in der EU in Verkehr gebrachten Produkten als auch auf die Anbieter damit verbundener Dienstleistungen sowie Nutzer der Produkte und Dienstleistungen anwendbar sein.

Darüber hinaus werden aber auch all diejenigen erfasst, die Daten austauschen und dabei einen Bezug zur EU haben – beispielsweise auch Dateninhaber mit Sitz in der Europäischen Union und solche aus Drittstaaten, die Daten an Empfänger in der EU weitergeben sowie Datenverarbeitungsdienste, die ihre Dienste an Kunden in der EU anbieten.

Unternehmen stehen hierbei vor der Herausforderung, zu beurteilen, ob ihre Produkte vom Anwendungsbereich des Entwurfs des Data Acts umfasst sind. Insoweit ist dringend eine frühzeitige Auseinandersetzung hiermit geboten. Auch aufgrund der Vielzahl an Produkten mit unterschiedlichen technischen Möglichkeiten und der teilweisen nur nuancenhaften Unterscheidbarkeit dieser, wird die Beurteilung der Eröffnung des Anwendungsbereichs nicht immer einfach zu beurteilen sein.

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 2022 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 2022 eingebunden.

Der Datenschutzbeauftragte wird im folgenden Jahr 2023 regelmäßig Abfragen durchführen, um eventuell neue oder geänderte Verfahren der Verarbeitung personenbezogener Daten frühzeitig zu identifizieren.

II. Dokumentation des Datenschutzes im Jahr 2022

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 15.11.2022 ein Jahresgespräch (in digitaler Form) mit der Prodware Deutschland AG, geführt. 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 wird 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.

Die DSGVO erfordert, dass die Auftragsverarbeiter-Liste komplett und aktuell ist. Alle notwendigen Muster-AVV liegen vor. Dem DSB liegt eine aktuelle AVV-Liste vor.

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

a) Verarbeitungsverzeichnis (VVZ) nach Art. 30 Abs. 1 DSGVO - ANLAGE 5) -

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 notwendigen VVZ wurden identifiziert und erstellt sowie im Jahr 2022 aktualisiert.

Hinweis des Datenschutzbeauftragten: Das Führen der Dokumentation im Datenschutz ist kein statisches Element, sondern ein dynamischer Prozess. Durch die laufende Rechtsprechung und Konkretisierungshinweise seitens der Datenschutzbehörden, sollte die Dokumentation stets auf dem aktuellen Stand gehalten werden.

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)

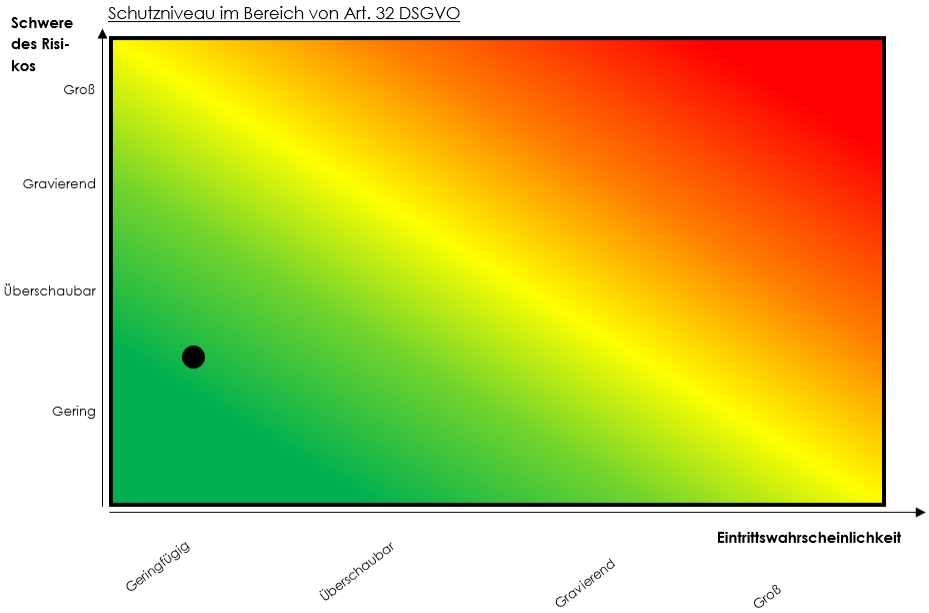
Art. 32 Abs. 1 DSGVO: Sicherheit der Verarbeitung

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 Technischen Organisatorischen Maßnahmen (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.

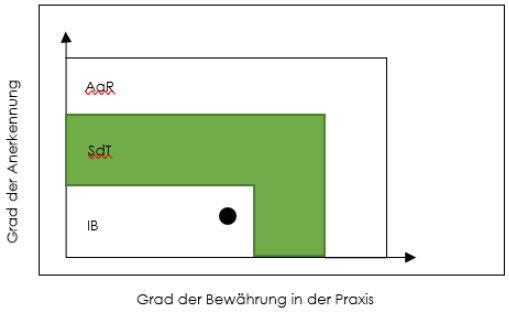
Ausgangspunkt bei der Bewertung der erforderlichen TOM muss immer eine Risikoanalyse bzw. die Betrachtung des erforderlichen Schutzniveaus sein (siehe **Bild 1**) sowie die Betrachtung des Stands der Technik im Bereich der implementierten Maßnahmen (siehe **Bild 2**).



(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. Ferner rücken die Anforderungen an die Dokumentation in den Vordergrund und - damit zusammenhängend - an die Nachweisbarkeit der getroffenen Maßnahmen und Kontrollen (vgl. Art. 5 Abs. 2 DSGVO). Auch hier gilt, die Maßnahmen sind nicht statisch, sondern sie müssen fortgeschrieben werden.

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 2022 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.

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 neues Schulungsprogramm wurde eingeführt. Jeder Mitarbeiter muss die Schulung durchführen und eine entsprechende Prüfung abschließen. Der Status der abgeschlossenen Schulungen liegt dem DSB vor.

Eine Auffrischungsschulung mit aktuellen Themen zur Entwicklung der Rechtsprechung innerhalb der DSGVO und den daraus erforderlichen Handlungsempfehlungen wird im Jahr 2023 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 2022 fanden zahlreiche Telefonate mit dem Datenschutzbeauftragten statt und es wurden zahlreiche Anfragen bearbeitet. Die geleistete Arbeit wurde dokumentiert.

12. Drittstaatenproblematik (Art. 44 - 50 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 2022 erfolgte eine Überprüfung der Drittlandthematik bei der Prodware Deutschland AG, welche die nachfolgenden Schritte bei der Übermittlung von personenbezogenen Daten in ein Drittland beachtet:

- 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 2022

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 2023

Die im Rubrum aufgeführten Parteien haben die weitere Zusammenarbeit, auch für den Berichtszeitraum 2023, beschlossen.

München, den 09.01.2023

Marcel Erntges
PRW Consulting GmbH