Datenschutz Jahresbericht 2024

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 ... 3

1. Kontaktdaten ... 3
2. Genereller Hinweis ... 5
3. Aufbau des Jahresberichtes ... 5

B. Besonderer Teil ... 6

I. Grundlagen ... 6

1. Genereller Rückblick auf 2024 und Ausblick auf 2025 ... 6
2. Datenschutzmanagement ... 13
3. Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO) ... 14
4. Einbindung des Datenschutzbeauftragten (Art. 39 DSGVO) ... 14

II. Dokumentation des Datenschutzes im Jahr 2024 ... 15

1. Jahresgespräch (Art. 39 Abs. 1 lit. a) DSGVO) ... 15
2. Informationspflichten / Betroffenenrechte (Art. 12 ff. DSGVO) ... 16
3. Vertraulichkeitsvereinbarung / Richtlinie ... 17
4. Löschkonzept - LK - (Art. 17 DSGVO) ... 17
5. Auftragsverarbeitung (Art. 28 DSGVO) ... 18
6. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 und Abs. 2 DSGVO) ... 18
7. Technische und Organisatorische Maßnahmen – TOM – (Art. 32 DSGVO) ... 19
8. Datenschutzverletzung (Art. 33 DSGVO) ... 21
9. Datenschutz-Folgenabschätzung - DSFA - (Art. 35 DSGVO) ... 22
10. Schulungs- / Sensibilisierungsmaßnahmen (Art. 39 DSGVO) ... 24
11. Anfragen intern / extern (Art. 39 DSGVO) ... 25
12. Drittstaatenproblematik (Art. 44 ff. DSGVO) ... 25
13. Fazit zu 2024 ... 27

C. Ausblick auf 2024 ... 27

1. Zusammenarbeit ... 27

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 2024 und Ausblick auf 2025

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. Ziel ist es, die Widerstandsfähigkeit der EU gegenüber Cyberbedrohungen zu stärken und gleichzeitig den freien Datenverkehr zu gewährleisten. Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese in nationales Recht überführen. In Deutschland findet die voraussichtlich letzte Lesung des Gesetzentwurfes im Februar 2025 statt.

Sie dient als rechtlicher Rahmen für den Schutz von Netz- und Informationssystemen in kritischen Sektoren wie beispielsweise Energie, Gesundheitswesen und Finanzwesen und ist erweitert worden um mehrere Branchen und es wird in wichtige und sehr wichtige Sektoren als auch Unternehmen unterschieden.

Die NIS-2-Richtlinie hat dabei Auswirkungen auch auf den Datenschutz, wenn es um die Sicherheit von Kommunikations- und Informationssystemen geht. 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 Unternehmen 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.

Es gilt zu prüfen, ob man als Unternehmen aktiv in den Erfassungsbereich von NIS-2 fällt oder passiv über die Lieferkette Kunde-Lieferant eingebunden wird.

b) Künstliche Intelligenz aus Sicht der DSGVO

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union stellt einen bedeutenden rechtlichen Rahmen dar, der den Schutz personenbezogener Daten gewährleistet. In einer Ära, in der künstliche Intelligenz (KI) zunehmend in verschiedenen Bereichen eingesetzt wird, sind die Anforderungen der DSGVO für Unternehmen und Organisationen besonders relevant. KI-Systeme, die oft große Mengen an Daten verarbeiten, müssen sicherstellen, dass sie die Datenschutzrechte der betroffenen Personen respektieren und die gesetzlichen Vorgaben einhalten.

Transparenz:

Eine der zentralen Anforderungen der DSGVO ist die Transparenz. Unternehmen müssen die betroffenen Personen klar und verständlich darüber informieren, wie ihre Daten verarbeitet werden. Dies umfasst Informationen über den Zweck der Datenverarbeitung, die Art der verarbeiteten Daten und die Empfänger dieser Daten. Beim Einsatz von KI bedeutet dies, dass die Algorithmen und deren Entscheidungen nachvollziehbar sein müssen. Die sogenannte "Black Box" der KI, bei der Entscheidungsprozesse intransparent sind, stellt hierbei eine besondere Herausforderung dar.

Rechtmäßigkeit:

Die DSGVO legt großen Wert auf die Rechtmäßigkeit der Datenverarbeitung. Es muss eine rechtliche Grundlage für die Verarbeitung personenbezogener Daten geben, wie beispielsweise die Einwilligung der betroffenen Person oder die Erfüllung eines Vertrags. Bei KI-Systemen ist es daher wichtig, sicherzustellen, dass die Datenverarbeitung auf einer soliden rechtlichen Basis erfolgt. Dies kann insbesondere bei der Sammlung von Trainingsdaten für maschinelles Lernen eine Herausforderung darstellen, da oft große Datenmengen aus verschiedenen Quellen zusammengeführt werden.

Datenminimierung:

Ein weiteres wichtiges Prinzip der DSGVO ist die Datenminimierung. Dies bedeutet, dass nur die Daten verarbeitet werden dürfen, die für den jeweiligen Zweck notwendig sind. Im Kontext von KI bedeutet dies, dass Unternehmen darauf achten müssen, nicht mehr Daten zu sammeln und zu speichern als unbedingt erforderlich. Darüber hinaus fordert die DSGVO, dass personenbezogene Daten nur so lange gespeichert werden, wie es für den jeweiligen Verarbeitungszweck notwendig ist. Dies erfordert klare Datenmanagement- und Löschkonzepte.

Rechte der Betroffenen:

Die DSGVO stärkt die Rechte der betroffenen Personen erheblich. Diese haben unter anderem das Recht auf Auskunft über die Verarbeitung ihrer Daten, das Recht auf Berichtigung unrichtiger Daten und das Recht auf Löschung ihrer Daten. Beim Einsatz von KI müssen Unternehmen sicherstellen,

dass diese Rechte gewahrt werden können. Dies bedeutet beispielsweise, dass die Systeme so gestaltet sein müssen, dass sie in der Lage sind, auf Anfragen zur Datenlöschung zu reagieren und die betroffenen Personen nicht diskriminieren.

Datensicherheit:

Schließlich fordert die DSGVO, dass geeignete technische und organisatorische Maßnahmen getroffen werden, um die Sicherheit der Daten zu gewährleisten. Bei KI-Systemen, die oft in großem Umfang Daten verarbeiten und speichern, ist die Datensicherheit von besonderer Bedeutung. Unternehmen müssen regelmäßige Risikobewertungen durchführen und sicherstellen, dass ihre Systeme gegen unbefugten Zugriff, Verlust oder Manipulation geschützt sind. Dies umfasst auch die Einführung von Verschlüsselungstechnologien und sicheren Authentifizierungsverfahren.

Fazit:

Zusammenfassend lässt sich sagen, dass die DSGVO beim Einsatz von künstlicher Intelligenz eine Vielzahl von Anforderungen stellt, die Unternehmen berücksichtigen müssen. Unabhängig davon müssen KI-Systeme im Einklang sein mit sonstigen einschlägigen Gesetzen wie zum Beispiel dem Urheberrecht oder dem AGG.

Wir können Sie hier als PRW-Group ganzheitlich im Bereich der Planung und Umsetzung der rechtlichen Anforderungen unterstützen. Gerne stellen wir Ihnen jederzeit unser Konzept zur rechtlich konformen Nutzung von künstlicher Intelligenz vor.

c) Urteile mit Datenschutzrelevanz

Auch im Jahr 2024 haben europäische und deutsche Gerichte aktuelle Urteile zum Schutz personenbezogener Daten getroffen. Folgende Entscheidungen sind für Unternehmen besonders relevant:

Gesundheitsdaten

In einem Urteil vom 4. Oktober 2024 (Rs. C-21/23) hat der Europäische Gerichtshof (EuGH) entschieden, dass der Begriff der Gesundheitsdaten weit auszulegen ist. Bereits der Verkauf von apothekenpflichtigen Medikamenten wie „Aspirin“ und „Grippostad“ stellt nach Auffassung des EuGH eine Verarbeitung besonders geschützter Gesundheitsdaten dar. Die Daten, die Kunden beim Kauf von Arzneimitteln angeben - Name, Lieferadresse und Angaben zum Medikament - sind nach Auffassung des Gerichts Gesundheitsdaten. Ihre Verarbeitung bedarf auch bei nicht verschreibungspflichtigen Arzneimitteln einer ausdrücklichen Einwilligung, da Rückschlüsse auf den Gesundheitszustand möglich sind. Eine "gewisse Wahrscheinlichkeit" reiche aus, so der EuGH. Ausgehend von dieser Argumentation wird es künftig noch schwerer möglich sein, eine konkrete Einschränkung von Art. 9 DSGVO zu argumentieren, d. h. der Begriff ist wesentlich weiter auszulegen als bisher.

Website / Cookie-Banner

Das OLG Köln stellte mit einem Urteil von Januar 2024 (6 U 80/23) klar, dass Cookie-Banner fair gestaltet sein müssen und Websitebesuchern eine echte Wahl lassen müssen, ob sie Cookies akzeptieren wollen oder nicht. Geklagt hatte eine Verbraucherschutzorganisation. Sie beanstandete, dass die erste Seite eines Cookie-Banners die Möglichkeit vorsehen muss, Cookies abzulehnen oder zu akzeptieren. Ebenso erfolgreich rügte sie eine Gestaltung, bei der neben dem Schriftzug „Akzeptieren und Schließen“ ein „X“ stand.

Das Gericht entschied, dass das Cookie-Banner der Beklagten nicht die Anforderungen nach DSGVO und Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) erfülle. Die Beklagte habe bei den Cookie-Bannern intransparente Designs verwendet. Die bloße Auswahl zwischen „Akzeptieren“ und „Einstellungen“ sei keine echte Wahl im Sinne der datenschutzrechtlichen Anforderungen an eine informierte Einwilligung. Betroffenen Personen würde durch die konkrete Gestaltung gerade keine gleichwertige Ablehnungsoption angeboten, weshalb sie zur Abgabe der Einwilligung hingelenkt und von der Ablehnung der Cookies angehalten werden, sodass die erteilte Einwilligung nicht als freiwillig und hinreichend aufgeklärt angesehen werden könne. Betroffene Personen könnten nämlich auf der ersten Ebene des Cookie-Banners zwar sofort zustimmen, möchten sie aber ablehnen, werden sie auf die zweite Ebene geleitet. Zudem sei das Feld „Akzeptieren“ in einem auffälligen Blau dargestellt, während die Einstellungen zum Ablehnen der Einwilligungserteilung in einem Grau dargestellt werden. Ferner werde auch auf der zweiten Ebene im selben Design

die Zustimmung der Einwilligung farblich hervorgehoben, während die Ablehnung manuell ausgeschaltet werden müsse (Cookie-Opt-out). Hinzutrete, dass im Layout auf der oberen rechten Seite ein X mit „Akzeptieren und speichern“ angebracht sei, dass den Eindruck erwecke, man könne die Einwilligung ablehnen. Daher verstoße auch die Gestaltung der Cookie-Banner mit dem verlinkten Button „Akzeptieren & Schließen X“ in der rechten oberen Ecke gegen die Grundsätze von Transparenz und Freiwilligkeit der Einwilligung.

Informationspflichten

Im vorliegenden Fall führte ein potenzieller Arbeitgeber eine Suchmaschinen-Recherche durch, um Informationen über den Bewerber zu erhalten. Das LAG Düsseldorf entschied Urteil vom 10.04.2024, Az. 12 Sa 1007/23, dass der Bewerber über diese Datenerhebung gemäß Art. 14 DSGVO zu informieren sei. Die Information über die Datenkategorien müsse dabei so präzise und spezifisch gefasst sein, dass die betroffene Person die Risiken abschätzen kann, die mit der Verarbeitung der erhobenen Daten verbunden sein können. Kommt der potenzielle Arbeitgeber dieser Informationspflicht nicht nach und verwertet dieser die erlangten Informationen im Stellenbesetzungsverfahren, steht dem Bewerber ein Entschädigungsanspruch gemäß Art. 82 Abs. 1 DSGVO zu. Vorliegend empfand das LAG Düsseldorf einen Schadenersatzanspruch in Höhe von 1.200 € für angemessen.

Schrems vs. Facebook

Ein Streit zwischen dem Datenschutzaktivisten Maximilian Schrems und Meta landete erneut vor dem Europäischen Gerichtshof (EuGH), Urt. v. 04.10.2024, Az. C-446/21. Es ging dabei um den Umfang, in dem Facebook (bzw. der Mutterkonzern „Meta“) personenbezogene Daten, insbesondere zur sexuellen Orientierung, für personalisierte Werbung nutzen darf. Schrems gab an, häufig Werbung erhalten zu haben, die gezielt homosexuelle Personen anspreche, sowie Einladungen zu Veranstaltungen, die sich an diese Zielgruppe richteten. Auf seinem Facebook-Profil fanden sich jedoch keine Hinweise auf seine sexuelle Orientierung. Diese hatte er lediglich im Rahmen einer öffentlichen Podiumsdiskussion öffentlich geäußert, nachdem er schon lange Zeit Nutzer von Facebook war. Schrems vertrat die Auffassung, dass diese Werbung das Ergebnis einer Analyse seiner Interessen sei, was er als unzulässig empfand. Daraufhin brachte er die Angelegenheit vor österreichische Gerichte. Der Oberste Gerichtshof in Österreich legte dem EuGH schließlich zwei Fragen zur Vorabentscheidung vor: Erstens sollte geklärt werden, ob Facebook gemäß der DSGVO personenbezogene Daten unbegrenzt für zielgerichtete Werbung analysieren und verarbeiten darf. Zweitens wollte das Gericht wissen, ob die öffentliche Äußerung von Schrems über seine Sexualität die Verarbeitung dieser Informationen für personalisierte Werbung rechtfertigt.

In Bezug auf die erste Frage betonte der EuGH den in der DSGVO festgelegten Grundsatz der Datenminimierung. Diesem stehe entgegen, wenn sämtliche personenbezogenen Daten "zeitlich un-

begrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden". Bisher haben Facebook und viele weitere Akteure im Bereich der Online-Werbung diese Regel einfach ignoriert und keine Löschfristen oder Beschränkungen nach Art der personenbezogenen Daten vorgesehen. Die Anwendung des „Grundsatzes der Datenminimierung“ schränkt die Verwendung personenbezogener Daten für Werbezwecke radikal ein. Der Grundsatz der Datenminimierung gilt unabhängig von der Rechtsgrundlage für die Verarbeitung. Somit können selbst dann, wenn ein Person in personalisierte Werbung eingewilligt hat, nicht auf unbestimmte Zeit ihre personenbezogenen Daten verwendet werden.

Auf die zweite Frage hin stellten die Luxemburger Richter klar: Wenn jemand von sich aus Informationen über seine sexuelle Orientierung öffentlich teilt, dürfen diese Daten zwar grundsätzlich verarbeitet werden. Das bedeute jedoch nicht, dass andere, zusätzlich gesammelte Informationen über die sexuelle Orientierung ebenfalls verarbeitet werden dürfen. Besonders wichtig sei dabei, dass Betreiber sozialer Netzwerke keine weiteren Daten von Drittanbietern nutzen, um durch Analyse und Aggregation personalisierte Werbung zu erstellen, auch wenn die Person ihre sexuelle Orientierung bereits öffentlich gemacht hat.

d) Datenschutzrechtlicher Schadensanspruch nach Cyberangriffen

Die Anzahl der Cyberangriffe steigt seit Jahren quantitativ und qualitativ kontinuierlich an. Regelmäßig werden personenbezogene Daten von Hackern erbeutet, die von Unternehmen als Verantwortliche verarbeitet werden. Nach den Cyberangriffen werden gegen die betroffenen Unternehmen Schadensersatzansprüche von den Betroffenen ausgesprochen.

Laut einer Studie von Bitkom waren 81 % der Unternehmen von Cyberangriffen 2023 betroffen, was zu einem wirtschaftlichen Schaden von 267 Mrd. Euro führte. 45 % der Angriffe kamen aus China, 39 % aus Russland. Für 2/3 der betroffenen Unternehmen ist der Cyberangriff existenzbedrohlich.

Mittlerweile haben diverse Rechtsanwaltskanzleien sich die datenschutzrechtlichen Schadensansprüche zu ihrem Geschäftsmodel gemacht, um groß angelegte und erfolgreiche Cyberangriffe zu identifizieren und Ansprüche der Betroffenen geltend zu machen. Der EuGH hat in letzter Zeit mehrere Urteile zum immateriellen Schadensanspruch nach Art. 82 DSGVO erlassen, die die Hürden zur Geltendmachung durch Betroffene gesenkt haben. Der EuGH hat zwar die Voraussetzungen zur Inanspruchnahme gesenkt, aber es ist davon auszugehen, dass nicht alle Schadenersatzansprüche Erfolg haben werden. Alle Anspruchsteller müssen ihren immateriellen Schaden darlegen und beweisen und die zuständigen Gerichte die subjektiven Empfindungen auf ihre Plausibilität hin überprüfen.

Ein Anknüpfungspunkt der Haftung für Unternehmen als datenschutzrechtliche Verantwortliche im Kontext von Cyberangriffen ist regelmäßig ein Verstoß gegen Art. 32 DSGVO (Sicherheit der Verarbeitung), für dessen Nichtvorliegen jetzt die Unternehmen darlegungs- und beweisbelastet sind.

Es ist dringendst zu empfehlen, dass die Unternehmen ihre technischen und organisatorischen Maßnahmen (TOM) im Hinblick auf die gesetzlichen Vorgaben nach Art. 32 DSGVO regelmäßig überprüfen und dokumentieren. Das Haftungsrisiko für Unternehmen als Anspruchsgegner ist entsprechend merklich gestiegen. Dieses Risiko könnte in der Zukunft durch innovative Möglichkeiten kollektiver Rechtsdurchsetzungen potenziert werden. Nur durch aktuelle, dem technischen Stand entsprechende technischen und organisatorischen Maßnahmen kann einer Haftung entgangen werden.

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 2024 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 2024 eingebunden.

Der Datenschutzbeauftragte wird im folgenden Jahr 2025 regelmäßig Abfragen durchführen, um eventuell neue oder geänderte Verfahren der Verarbeitung personenbezogener Daten frühzeitig zu identifizieren.

II. Dokumentation des Datenschutzes im Jahr 2024

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 10.07.2025 ein Jahresgespräch (in digitaler Form) mit diversen Ansprechpartnern 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 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 2024 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.

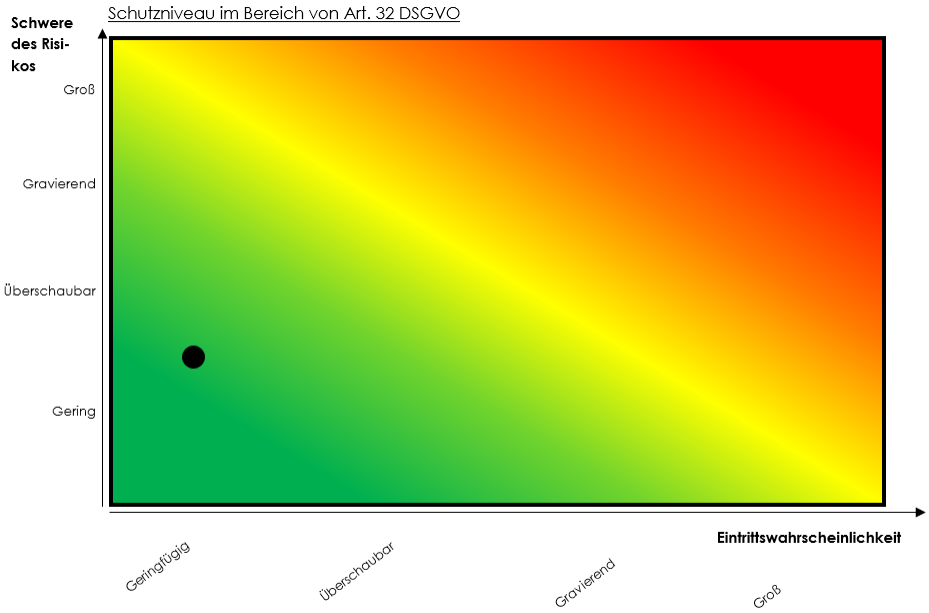
7. Technische und Organisatorische Maßnahmen – TOM – (Art. 32 DSGVO)

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.

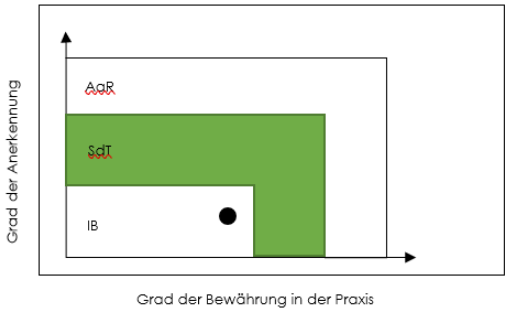
Grundsätzlich steht es jedem Verantwortlichen frei, selbst diejenigen TOM auszuwählen, die passend zu der eigenen Art der Verarbeitung und Unternehmensgröße sind, sofern damit ein wirksames angemessenes Schutzniveau erreicht werden kann. Die DSGVO, als auch die Aufsichtsbehörden, fordern jedoch verstärkt 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. 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, sie müssen fortgeschrieben werden.

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 2024 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 2024 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 2025 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 2024 fanden zahlreiche Telefonate mit dem Datenschutzbeauftragten statt und es wurden zahlreiche Anfragen bearbeitet. Die geleistete Arbeit wurde dokumentiert. Ausgetauschte E-Mails werden nach Ablauf der Löschfrist gelöscht.

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 2024 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 2024

Die Anforderungen der DSGVO und des BDSG sind im Wesentlichen 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 2025, beschlossen.

München, den 29.07.2025

Marcel Erntges
PRW Consulting GmbH