

Datenschutz Jahresbericht 2020

Proeware Deutschland AG

Notkestr. 7

22607 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
4.	Genereller Rückblick auf 2020	6
B.	Besonderer Teil	7
I.	Datenschutzrechtliche Aktivitäten im Jahr 2020	7
1.	Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO)	7
2.	Datenschutzmanagement	7
3.	Einbindung des Datenschutzbeauftragten (Art. 39 DSGVO)	8
4.	Schulungs- / Sensibilisierungsmaßnahmen (Art. 39 DSGVO)	9
5.	Anfragen intern / extern (Art. 39 DSGVO)	9
6.	Jahresgespräch	9
II.	Dokumentation des Datenschutzes im Jahr 2020	11
1.	Informationspflichten / Betroffenenrechte (Art. 12 ff. DSGVO)	11
2.	Arbeitsrechtliche Maßnahmen im Rahmen der DSGVO	12
3.	Auftragsverarbeitung (Art. 28 DSGVO)	13
4.	Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)	14
5.	Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DSGVO -	15
6.	Löschkonzept (Art. 5, 17 DSGVO)	18
7.	Technische und Organisatorische Maßnahmen (TOMs) - Art. 32 DSGVO -	18
8.	Datenschutzverletzung (Art. 33 DSGVO)	20
9.	Drittstaatenproblematik (Art. 44 ff. DSGVO)	21
10.	Website-Check	21
C.	Ergebnis der Datenschutzprüfung 2020	22
1.	Zusammenfassung	22

A. Allgemeiner Teil

1. Kontaktdaten

Auftraggeber als verantwortliche Stelle oder als Verantwortlicher

Name	Prodware Deutschland AG		
Straße / Ort	Notkestr. 7 / 22607 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
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
George Knap	Managing Director Prodware Czech Republic sro / Prodware Georgia LLC / DPO Prodware Group	+420 585 242 854	g.knap@prodwaregroup.com

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
Prof. Dr. Johannes Caspar	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

Der Jahresbericht gibt den Sachstand zum Datenschutz im angegebenen Berichtsjahr wieder. 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: 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 und der IT-Sicherheit bei der ProWare Deutschland AG. Der Bericht erläutert außerdem bereits erfolgte und geplante Anpassungen von Aktivitäten und Dokumentationen im Datenschutz.

4. Genereller Rückblick auf 2020

a) Pandemie Covid-19 (Corona) und die Auswirkungen

Der erste Covid-19 (SARS-CoV-2) Fall ereignete sich im Kreis Starnberg am 27. Januar 2020 (Webasto). In Heinsberg wurde im Februar 2020 Karneval gefeiert. Dann hat es uns alle mehr oder weniger „erwischt“. Es kam zu ersten Lockdowns. Die Empfehlungen der Politik, wie mit der Pandemie umgegangen werden sollte, wer und was wie unterstützt oder gefördert werde, waren nicht immer stimmig und einheitlich. Viele Unternehmen, die dem Home-Office Gedanken bis dahin eher skeptisch gegenüberstanden, sahen sich in der Pflicht, das Thema aufzunehmen, um Schutzmaßnahmen für Leib und Leben zu ergreifen. Dies bedeutete für viele - von heute auf morgen - die nicht vorbereitete Umstellung auf das Home-Office und somit auf die Digitalisierung. Die Kommunikation wurde auf digital umgestellt. Der Datenschutz spielte hier zunächst eine untergeordnete Rolle. Bis auf wenige Ausnahmen verhielten sich die Datenschutzbehörden sehr kooperativ und konstruktiv, auch wenn die Behörden natürlich insgesamt nicht von ihren Pflichten entbunden wurden. Will heißen: Prüfungen / Kontrollen / Verhängung von Bußgeldern wurde zunächst zurückgestellt. Sie sind jedoch nicht aufgehoben.

b) Schrems II

Und, als wäre die Pandemie noch nicht genug, entscheidet der Europäische Gerichtshof (EuGH) im Urteil vom 16. Juli 2020 in der Rechtssache C-311/18: Es ergeht das sog. „Schrems II“ Urteil. Was folgt ist eine Unzahl von Statements und Kommentierungen von Aufsichtsbehörden, Anwaltskanzleien und sonstigen, die sich berufen fühlten, die Entscheidung zu kommentieren. Bemerkenswert an den meisten Veröffentlichungen ist, dass das Einzige, was nach ihrem Genuss übrigbleibt, Ratlosigkeit ist. Spannt man den Bogen weiter (europäisch) auf, sieht das Ganze noch verrückter aus. Da gibt es Länder, wie Dänemark oder Spanien, die sehen die Entscheidung eher gelassen. Sie appellieren für ein europäisch abgestimmtes Vorgehen. Andere - und leider viele deutsche Aufsichtsbehörden - sehen das nicht so locker. Sie fordern z. T. ein Verbot von Microsoft Produkten. Wie das wohl auf die Nutzer im Home-Office oder auf die Bereitsteller von IT-Infrastruktur wirkt? Sachlichkeit ist gefragt. Ob eine Applikation rechtskonform eingesetzt wird, ist im Einzelfall zu prüfen. Pauschale Verurteilungen mit Produktverböten helfen nicht. Wir haben die neuesten Empfehlungen der europäischen Datenschutzbehörden (EDSA) analysiert und können Lösungen aufzeigen. Wer hier Unterstützung möchte, den unterstützen wir auch (siehe Empfehlungen).

Die vorstehenden Punkte und dabei insbesondere die Pandemie, haben sehr viele Unternehmen, Einrichtungen, Mitarbeiter und Bürger betroffen. Sie haben auch die Zusammenarbeit

mit dem Datenschutzbeauftragten gezeichnet. Aus den gemeinsam geschätzten Vor-Ort-Terminen wurden virtuelle Termine. Das hat, bei aller Krise, ganz gut funktioniert. Vielen Dank dafür.

B. Besonderer Teil

I. **Datenschutzrechtliche Aktivitäten im Jahr 2020**

1. **Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO)**

Art. 37 Abs. 1 b) DSGVO: 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.

2. **Datenschutzmanagement**

Die DSGVO verpflichtet die verantwortliche Stelle nicht ausdrücklich, ein Datenschutzmanagement einzuführen, das den Schutz der personenbezogenen Daten sicherstellen soll. Gleichwohl wird derjenige, der den Datenschutz ernsthaft umsetzen und implementieren möchte, auf ein solches System nicht verzichten können, weil das „Handling“ des modernen Datenschutzes in einer Vielzahl von Vorschriften geregelt ist, 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 **Technische und Organisatorische Maßnahmen (TOMs)** umzusetzen 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 (nachfolgend kurz „PRW“) hat, gemeinsam mit dem Auftraggeber, ein solches System bei der Prodware Deutschland AG eingeführt.

Dieser Datenschutzbericht zeigt auf, wie die verantwortliche Stelle, gemeinsam mit dem Datenschutzbeauftragten, die Datenschutzanforderungen im Jahr 2020 gemanagt haben.

3. Einbindung des Datenschutzbeauftragten (Art. 39 DSGVO)

Art. 39 DSGVO

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

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;

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;

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

d) Zusammenarbeit mit der Aufsichtsbehörde;

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.

(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 2020 eingebunden.

Der Datenschutzbeauftragte wird im folgenden Jahr 2021 regelmäßig Abfragen durchführen, um eventuell neue oder geänderte Verfahren der Verarbeitung personenbezogener Daten frühzeitig zu identifizieren.

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

Art. 39 Abs. 1 b) DSGVO: Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.

Alle Bestandsmitarbeiter wurden bei der Prodware Deutschland AG bereits geschult. Die Schulungen sind wie folgt organisiert:

- Basic DSGVO;
- Role Specific HR / Marketing / Service Delivery / etc.

Die Teilnahme an der Schulung wird mit einem Online-Test abgeschlossen. Diese Schulungen werden in regelmäßigen Intervallen wiederholt. Der Schulungsgrad ist als hoch zu bezeichnen.

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

Art. 39 Abs. 1 a) DSGVO: 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 2020 fanden Telefonate/Gespräche mit dem Datenschutzbeauftragten. Die entsprechenden Aktivitäten wurden dokumentiert.

6. Jahresgespräch

Der Datenschutzbeauftragte hat am 03.11.2020 ein Jahresgespräch (aufgrund der Pandemie Situation in digitaler Form) mit der Prodware Deutschland AG geführt. Folgende wesentliche Ergebnisse wurden darin festgehalten:

Prüfung der bestehenden AVV und VVZ

AVV: Im Kunden-Bereich wurden bis zum Tag des Gesprächstermins insgesamt fünfhundertsiebenunddreißig (537) AVV abgeschlossen, bei denen die Prodware Deutschland AG als Auftragsverarbeiter agiert.

VVZ: Bei der Prodware Deutschland AG werden Anzahl und Bearbeitungsstand aller VVZ regelmäßig geprüft und neue Verfahren aufgenommen. Für Verfahren und Bereiche, die global für die gesamte Prodware Group und somit auch für die Prodware Deutschland AG mitgelten, liegt eine zentrale Dokumentation vor.

Informationspflichten

Alle Informationspflichten wurden erstellt und sind derzeit aktuell.

Löschkonzept

Für die Prodware Group besteht konzernweit eine Data Retention Policy, in der beschrieben wird, dass alle personenbezogenen Daten nach Ablauf der jeweils vor Ort geltenden gesetzlichen Aufbewahrungsfristen zu löschen sind.

Technische und organisatorische Maßnahmen (TOMs)

Die TOMs sind beschrieben. Zur Evaluierung der bestehenden Maßnahmen kann auf die bestehenden Risikoeinschätzungen der Prodware Group zurückgegriffen werden.

II. Dokumentation des Datenschutzes im Jahr 2020

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

Auszüge:

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).

Erfolgt die Erhebung nicht beim Betroffenen, ist dieser innerhalb einer angemessenen Frist, spätestens aber nach einem (1) Monat, zu informieren. Werden die Daten zur Kommunikation mit der betroffenen Person verwendet, besteht die Informationspflicht jedoch direkt bei Kontaktaufnahme. 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.

Im Falle, dass die personenbezogenen Daten nicht beim Betroffenen erhoben werden, muss grundsätzlich der Informationspflicht nachgekommen werden. Nur in Ausnahmefällen ist dies nicht erforderlich, etwa, wenn dies unmöglich oder unverhältnismäßig aufwendig ist, die Erhebung und / oder Übermittlung gesetzlich vorgeschrieben ist, ein Berufsgeheimnis oder eine sonstige satzungsmäßige Geheimhaltungspflicht besteht. Der Gesetzgeber hat den Informationspflichten somit einen hohen Stellenwert eingeräumt.

Alle datenschutzrechtlichen Aktivitäten der verantwortlichen Stelle und des Datenschutzbeauftragten wurden dokumentiert. Aufgrund der Relevanz der Dokumentation wird diese nachfolgend nochmals gesondert ausgewiesen. Dabei kann es zu Redundanzen mit den beschriebenen Aktivitäten kommen.

2. Arbeitsrechtliche Maßnahmen im Rahmen der DSGVO

Zur Sicherstellung der arbeitsrechtlichen Aspekte wurde für die Prodware Deutschland AG ein Kurzgutachten von PRW Rechtsanwälte erstellt. Dieses liegt der verantwortlichen Stelle vor.

a) Betroffenenrechte

Die Beschäftigten sowie die Bewerber wurden darüber informiert werden, zu welchen Zwecken ihre personenbezogenen Daten erhoben werden, wer Datenschutzbeauftragter ist, an welche Empfänger die Daten gehen und welche Betroffenenrechte die Arbeitnehmer nach der DSGVO haben.

b) Vertraulichkeit (Verpflichtungserklärung)

Die Beschäftigten wurden nach den Vorschriften der DSGVO auf den Datenschutz verpflichtet. Insbesondere aus der besonderen Rechenschaftspflicht nach der DSGVO ergibt sich, dass eine Neubelehrung der Arbeitnehmer auf den Datenschutz sinnvoll ist, da diese die Bemühungen des Arbeitgebers zur Umsetzung der DSGVO manifestiert. Auch wenn sich letztlich nur die Vorschriften ändern und sich die Verpflichtung nach Art. 28 Abs. 3 lit. b DSGVO nur mittelbar ergibt, wurde die bisherige Verpflichtung zur Vertraulichkeit angepasst und an alle Beschäftigten ausgegeben.

3. Auftragsverarbeitung (Art. 28 DSGVO)

Art. 28 Abs. 3 Satz 1 DSGVO: 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 Sichtung und Prüfung der Auftragsverarbeitungsverträge (AVV) brachte folgende Ergebnisse:

Im Kunden-Bereich wurden bis zum Tag des Gesprächstermins insgesamt fünfhundertsiebenunddreißig (537) AVV abgeschlossen, bei denen die Prodware Deutschland AG als Auftragsverarbeiter agiert.

Im Bereich der Dienstleister wurden alle zweiundzwanzig (22) Unternehmen mit einem AVV verpflichtet.

4. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Art. 30 Abs. 1 Satz 1 DSGVO: Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.

Bei der Prodware Deutschland AG werden Anzahl und Bearbeitungsstand aller VVZ regelmäßig geprüft und neue Verfahren aufgenommen. Für Verfahren und Bereiche, die global für die gesamte Prodware Group und somit auch für die Prodware Deutschland AG mitgelten, liegt eine zentrale Dokumentation vor.

- Bei der Prodware Deutschland AG wurden Anzahl und Bearbeitungsstand von allen bekannten VVZ am 03.11.2020 geprüft.

Weitere VVZ werden folgen, wenn neue Verfahren, bzw. Prozesse mit personenbezogenen Daten, eingeführt werden.

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

Art. 35 Abs. 1 und 2 DSGVO:

(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.

(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.

Nachfolgend eine detaillierte Erläuterung der deutschen Aufsichtsbehörden (gemäß Art. 35 DSGVO; § 67 BDSG). 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 substantziellen 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.

Für Verfahren, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen, wurde ein Konzept entwickelt. Dieses Konzept ermöglicht es der Prodware Deutschland AG einen Vorgang anzustoßen, um eine entsprechende Abschätzung durchzuführen.

6. Löschkonzept (Art. 5, 17 DSGVO)

Art. 5 Abs. 1 e) DSGVO: 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 a) DSGVO: 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.

Für die Prodware Group besteht konzernweit eine Data Retention Policy, in der beschrieben wird, dass alle personenbezogenen Daten nach Ablauf der jeweils vor Ort geltenden gesetzlichen Aufbewahrungsfristen zu löschen sind.

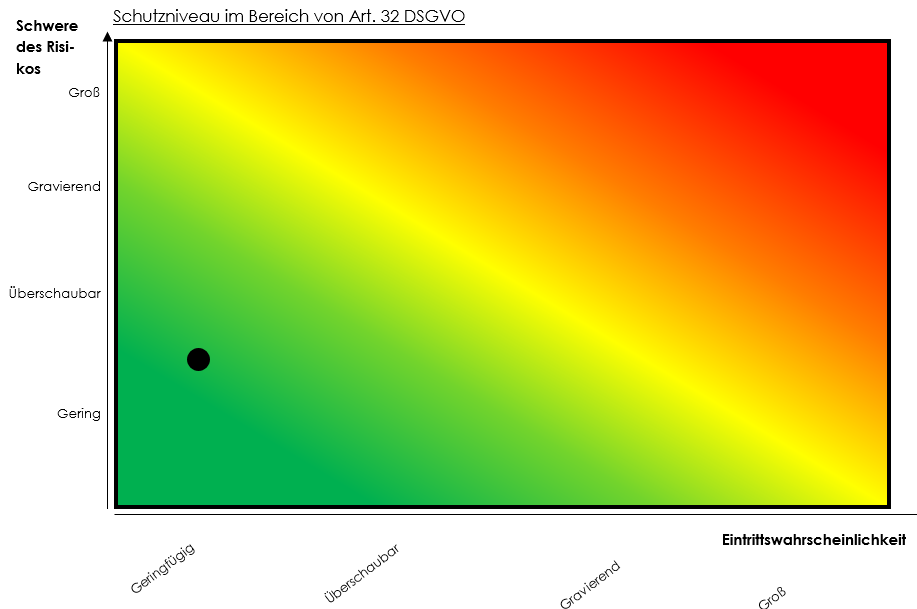
7. Technische und Organisatorische Maßnahmen (TOMs) - Art. 32 DSGVO -

Art. 32 Abs. 1 DSGVO: 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 TOMs 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 „Standes der Technik“ von TOMs. 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 Standes der Technik ein angemessenes Schutzniveau gewährleistet wird.

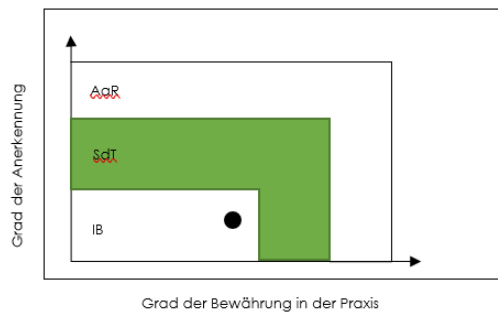
Ausgangspunkt bei der Bewertung der erforderlichen TOMs muss immer eine Risikoanalyse bzw. die Betrachtung des erforderlichen Schutzniveaus sein (siehe **Bild 1**) sowie die Betrachtung des Standes der Technik im Bereich der implementierten Maßnahmen (siehe **Bild 2**).



(Bild 1 Bewertung des Schutzniveaus)

Bestimmung des Technologiestandes Stand der Technik (ScT) Interne Bewertung (IB) Allg. anerkannte Regeln (AqR)

Einordnung des Technologiestandes



(Bild 2 Bestimmung des Technologiestandes)

In den Vordergrund rücken ferner die Anforderungen an die Dokumentation und - damit zusammenhängend - an die Nachweisbarkeit der getroffenen Maßnahmen und Kontrollen (vgl. Art. 5 Abs. 2 DSGVO).

Die TOMs sind beschrieben. Zur Evaluierung der bestehenden Maßnahmen kann auf die bestehenden Risikoeinschätzungen der Prodware Group zurückgegriffen werden.

8. Datenschutzverletzung (Art. 33 DSGVO)

Art. 33 Abs. 1 DSGVO: 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 Artikel 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 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.

- Es wurde ein Reaktionsplan zur Fristwahrung bei Datenpannen erarbeitet und bei der Prodware Deutschland AG bekannt gemacht. Dabei wurden bestimmte Rollen konkreten Personen zugewiesen. So soll sichergestellt sein, dass bei einem Datenschutzvorfall die zuständigen Mitarbeiter wissen, was zu tun ist.
- 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. Drittstaatenproblematik (Art. 44 ff. DSGVO)

Art. 44 ff. 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 Daten-übermittlung in ein Drittland muss zunächst überprüft werden, ob - unabhängig von den in den Art. 45 ff. DSGVO geregelten spezifischen Anforderungen an Datenübermittlungen in Dritt-länder - 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 Ver-arbeitung nichts entgegen, müssen gemäß Art. 44 DSGVO zusätzlich die spezifischen Anfor-derungen 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 empfan-gende Stelle im Drittland (Art. 44 Satz 1 2. HS DSGVO).

- Im Jahr 2020 erfolgte eine Überprüfung der Drittlandthematik.
- Die Drittlandthematik wurde in den Workshops und in den Schulungen mehrfach be-sprochen.
- Für diese Prodware Gesellschaften wurden die EU Model Clauses in das Intercompany Agreement mitaufgenommen.

10. Website-Check

Eine kursorische Prüfung der Website <https://www.prodwaregroup.com> wurde aufgrund der Neugestaltung der Website durchgeführt

Die Ergebnisse wurden der Prodware Deutschland AG gesondert mit einer rechtskonformen Datenschutzerklärung sowie einem Dokument über Widerspruchsmöglichkeiten (Cookie- und Opt Out Hinweise) übergeben.

C. Ergebnis der Datenschutzprüfung 2020

1. Zusammenfassung

Die Proware Deutschland AG und die Verantwortlichen handeln nach Kenntnis des Datenschutzbeauftragten im Berichtszeitraum 2020 im Rahmen der gesetzlichen Vorgaben der DSGVO.

München, 15. Januar 2021



Marcel Erntges
Datenschutzbeauftragter

Bitte beachten Sie:

Dieser Bericht ist ausschließlich für den Auftraggeber bestimmt. Ohne unsere Genehmigung ist es nicht gestattet, dieses Dokument oder Teile daraus in irgendeiner Form durch Fotokopie oder ein anderes Verfahren zu vervielfältigen und an unberechtigte Dritte zu verbreiten.
Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

© Copyright 2020 PRW Consulting GmbH