

## Datenschutz Jahresbericht 2021

**windata GmbH & Co.KG**

Gegenbaurstraße 4

88239 Wangen im Allgäu



PRW Consulting GmbH • Leonrodstraße 54 • D-80636 München • Tel: +49 89 210977-70  
Fax: +49 89 210977-77 • [info@prw-consulting.de](mailto:info@prw-consulting.de) • [www.prw-consulting.de](http://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

<b>A.</b>	<b>Allgemeiner Teil .....</b>	<b>3</b>
1.	Kontaktdaten .....	3
2.	Genereller Hinweis .....	5
3.	Aufbau des Jahresberichtes .....	5
4.	Genereller Rückblick auf 2021 .....	6
<b>B.</b>	<b>Besonderer Teil.....</b>	<b>8</b>
<b>I.</b>	<b><i>Datenschutzrechtliche Aktivitäten im Jahr 2021</i> .....</b>	<b>8</b>
1.	Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO) .....	8
2.	Datenschutzmanagement.....	8
3.	Einbindung des Datenschutzbeauftragten (Art. 39 DSGVO) .....	9
4.	Schulungs- / Sensibilisierungsmaßnahmen (Art. 39 DSGVO) .....	10
5.	Anfragen intern / extern (Art. 39 DSGVO) .....	10
6.	Jahresgespräch .....	11
<b>II.</b>	<b><i>Dokumentation des Datenschutzes im Jahr 2021</i> .....</b>	<b>12</b>
1.	Informationspflichten / Betroffenenrechte (Art. 12 ff. DSGVO) .....	12
2.	Arbeitsrechtliche Maßnahmen im Rahmen der DSGVO.....	13
3.	Auftragsverarbeitung (Art. 28 DSGVO).....	14
4.	Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) .....	14
5.	Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DSGVO - .....	16
6.	Löschkonzept (Art. 5, 17 DSGVO) .....	18
7.	Technische und Organisatorische Maßnahmen (TOM) - Art. 32 DSGVO - .....	19
8.	Datenschutzverletzung (Art. 33 DSGVO) .....	20
9.	Drittstaatenproblematik (Art. 44 ff. DSGVO) .....	21
10.	Website-Check .....	22
11.	Fazit zu 2021 .....	22
<b>C.</b>	<b>Ausblick auf 2022 .....</b>	<b>23</b>
1.	Zusammenarbeit .....	23
2.	Gesetzliche Neuerungen .....	23
3.	Empfehlungen für 2022.....	<b>Fehler! Textmarke nicht definiert.</b>

## A. Allgemeiner Teil

### 1. Kontaktdaten

#### Auftraggeber als verantwortliche Stelle oder als Verantwortlicher

<b>Name</b>	windata GmbH & Co. KG		
<b>Straße / Ort</b>	Gegenbaurstraße 4 / 88239 Wangen im Allgäu		
<b>Telefon / Fax</b>	+49 7522 9770-0 / +49 7522 9770-179		
<b>Internet / E-Mail</b>	www.windata.de / info@windata.de		
<b>Ansprechpartner</b>	<b>Funktion</b>	<b>Telefon</b>	<b>E-Mail</b>
Michael Rudhart	Geschäftsführer	+49 7522 9770-0	MichaelRudhart@windata.de
Ina Roth	stellvertretende Datenschutz-beauftragte	+49 7522 9770-0	InaRoth@windata.de

#### Auftragnehmer des Mandats externer Datenschutzbeauftragter

<b>Name</b>	PRW Consulting GmbH		
<b>Straße / Ort</b>	Leonrodstraße 54 / 80636 München		
<b>Telefon / Fax</b>	+49 89 210977-70 / +49 89 210977-77		
<b>Internet / E-Mail</b>	www.prw-consulting.de / info@prw-consulting.de		
<b>Ansprechpartner</b>	<b>Funktion</b>	<b>Telefon</b>	<b>E-Mail</b>
RA 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**

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

**Zuständige Aufsichtsbehörde**

<b>Name</b>	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg		
<b>Straße / Ort</b>	Lautenschlagerstraße 20 / 70173 Stuttgart		
<b>Telefon / Fax</b>	+49 711 615541-0 / +49 711 615541-15		
<b>Internet / E-Mail</b>	www.baden-wuerttemberg.datenschutz.de / poststelle@lfdi.bwl.de		
<b>Ansprechpartner</b>	<b>Funktion</b>	<b>Telefon</b>	<b>E-Mail</b>
Dr. Stefan Brink	Landesbeauftragter	+49 711 615541-0	poststelle@lfdi.bwl.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 bei der windata GmbH & Co. KG.

Der Bericht erläutert außerdem bereits erfolgte und geplante Anpassungen von Aktivitäten und Dokumentationen im Datenschutz. Er endet mit Empfehlungen und Optionen für das Jahr 2022.

## 4. Genereller Rückblick auf 2021

### a) BREXIT

Das Vereinigte Königreich wurde durch den Brexit zu einem Drittland, in das personenbezogene Daten aus der Europäischen Union nur exportiert werden durften, wenn dort ein vergleichbares Datenschutzniveau vorliegt oder geeignete Garantien für den Schutz der betroffenen Personen getroffen wurden. Die Europäische Kommission hat einen Angemessenheitsbeschluss für das Vereinigte Königreich am 28. Juni 2021 erlassen, wodurch dieses nunmehr als sicheres Drittland nach der DSGVO gilt. Der Abschluss von EU-Standardvertragsklauseln oder sonstiger geeigneter Garantien gem. Art. 46 DSGVO ist mit Dienstleistern, die ihren Sitz im Vereinigten Königreich haben, nun erstmal nicht erforderlich. Dennoch sollte die Wirksamkeit des Angemessenheitsbeschlusses jederzeit beobachtet werden, da dieser durch das Eingreifen der Europäischen Kommission oder mit Ablauf der Vier(4)-Jahres-Frist (2025) außer Kraft treten kann.

### b) EU-Standardvertragsklauseln

Am 04. Juni 2021 hat die EU-Kommission die neuen EU-Standardvertragsklauseln (SCC) 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:** Modul EINS betrifft die Übermittlung von personenbezogenen Daten zwischen zwei (2) Verantwortlichen.
- **Modul ZWEI:** Modul ZWEI bildet die Datenübermittlung vom Verantwortlichen an den Auftragsverarbeiter ab.
- **Modul DREI:** Modul DREI ist zu verwenden bei einer Datenübermittlung zwischen zwei (2) Auftragsverarbeitern.
- **Modul VIER:** Modul VIER hingegen bildet den Datentransfer von Auftragsverarbeitern an Verantwortliche ab.

Die modernisierten SCC ersetzen die unter der vorherigen Datenschutzrichtlinie 95/46 verabschiedeten SCC. Verantwortliche und Auftragsverarbeiter müssen ihre bestehenden Verträge und Vertragsverhältnisse prüfen und die neuen SCC abschließen. Die neuen Klauseln lösen allerdings nicht die Problematik der Einzelfallprüfung (Schrems II), da laut EuGH ggfs. zusätzliche Schutzmaßnahmen implementiert werden müssen.

Die überarbeiteten SCC schreiben so erstmals Garantien vor, „um etwaige Auswirkungen der Gesetze des Bestimmungs Drittlands“ auf die Einhaltung der Klauseln durch den Datenimporteur zu regeln. Dabei gilt es vor allem 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, nicht im Widerspruch zu den Klauseln stehen.

Die datenexportierenden Unternehmen kommen auch auf Grundlage der neuen SCC nicht umhin, für sämtliche auf SCC gestützte Übermittlungen im Einzelnen zu prüfen, ob nationales Recht im Drittland zu einer Untergrabung der Rechte und Freiheiten von Betroffenen führt und somit zusätzliche Maßnahmen für den Schutz der personenbezogenen Daten notwendig sind. Hierzu ist es dringend zu empfehlen, die konkreten Datentransfers im Einzelnen zu analysieren und festzustellen, welche Gesetze des Drittlandes jeweils Anwendung finden.

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.

### **c) Stand Schrems Urteil**

Mit Fragebögen überprüfen die Datenschutzaufsichtsbehörden länderübergreifend die Umsetzung der Schrems II Entscheidung des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 (Rechtssache C-311/18, „Schrems II“) in Unternehmen. Mit seiner Entscheidung hat das Gericht das EU-US-Privacy Shield für ungültig erklärt. Durch das Schrems II Urteil soll der Datenschutz der EU-Bürger beim Datentransfer in die USA und andere Drittländer weiter gestärkt werden.

Das neue „Schrems III“-Verfahren vor dem EuGH soll die Frage klären, welche rechtlichen Verhältnisse zwischen Facebook und den NutzerInnen herrschen. Der Konzern nutzt persönliche Daten seiner NutzerInnen nicht nur für den Betrieb des sozialen Netzwerkes, sondern auch für personalisierte Werbung. Seit Mai 2018 argumentiert Facebook, dass die NutzerInnen einen „Vertrag“ mit dem Konzern abgeschlossen hätten und dadurch sei keine „Einwilligung“ im Sinne der DSGVO notwendig. Rechtlich macht dies einen Unterschied, da eine Einwilligung jederzeit für die Zukunft widerrufen werden kann. Durch den Widerruf der Einwilligung der NutzerInnen wird die Zustimmung zur Verwendung von Daten für Werbung entzogen.

Das EU-Gericht soll auch die Frage zum Werbe-Targeting klären. Des Weiteren geht es darum, ob Facebook die Daten gezielt nach besonders sensiblen Kategorien - wie politischer Überzeugung und sexueller Orientierung - durchsuchen und filtern darf.

## B. Besonderer Teil

### I. Datenschutzrechtliche Aktivitäten im Jahr 2021

#### 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 windata GmbH & Co. KG 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 **T**echnische und **O**rganisatorische **M**aßnahmen (TOM) 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 (PRW) hat, gemeinsam mit dem Auftraggeber, der windata GmbH & Co. KG ein solches System eingeführt.



Dieser Datenschutzbericht zeigt auf, wie die verantwortliche Stelle, gemeinsam mit dem Datenschutzbeauftragten, die Datenschutzanforderungen im Jahr 2021 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 2021 eingebunden.

Der Datenschutzbeauftragte wird im folgenden Jahr 2022 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.*

Eine neue Datenschutzschulung ist für dieses Jahr bereits geplant.

#### 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 2021 fanden diverse Telefonate mit dem Datenschutzbeauftragten statt. Die Aktivitäten wurden dokumentiert.

## 6. Jahresgespräch

Der Datenschutzbeauftragte hat am 05. August 2021 das Jahresgespräch 2021 (in digitaler Form) mit der windata GmbH & Co. KG geführt. Folgende wesentliche Ergebnisse wurden darin festgehalten:

### **Auftragsverarbeitungsverträge (AVV)**

Der AVV enthält alle gesetzlichen Anforderungen gem. Art. 28 DSGVO.

### **Datenschutz-Folgenabschätzung (DSFA)**

Die DSFA wurden datenschutzkonform erstellt. Bei allen DSFA konnte nach der Umsetzung und dem Testen der Maßnahmen kein hohes Risiko mehr festgestellt werden.

Zusätzlich wurde für alle Verfahren eine generelle Schwellenwertanalyse durchgeführt, um festzustellen, welche Verfahren ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.

### **Informationspflichten**

Es wurden alle erforderlichen Informationspflichten gem. Art. 13 und 14 DSGVO für die folgenden Betroffenen erstellt:

- Mitarbeiter
- Kunden
- Bewerber

Alle Informationspflichten enthalten die notwendigen DSGVO-Anforderungen und sind leicht verständlich sowie jederzeit für die Betroffenen ersichtlich.

### **Vertraulichkeitsvereinbarung / Richtlinien**

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.

### **Technische und organisatorische Maßnahmen (TOM)**

Die TOM für Kunden im Bereich der Auftragsverarbeitung entsprechen den DSGVO-Anforderungen und dem Stand der Technik.

### **Verarbeitungsverzeichnisse (VVZ)**

Die VVZ wurden mit Hilfe der Muster von PRW erstellt bzw. ergänzt. Sie entsprechen den gesetzlichen Anforderungen.

### **Löschkonzept**

Die Löschfristen für die einzelnen Verarbeitungen wurden gem. DIN 66398 dokumentiert. Diese Dokumentation erfüllt die Anforderungen gem. Art. 17 DSGVO.

## **II. Dokumentation des Datenschutzes im Jahr 2021**

### **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**

### **a) Betroffenenrechte**

Die Beschäftigten sowie die Bewerber sollen 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. Die Erstellung eines Informationsblattes nach der DSGVO ist hierzu erforderlich.

Alle Bestandsmitarbeiter wurden bei der windata GmbH & Co. KG bereits geschult.

### **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 ist der Auftragsverarbeitungsvertrag in die Vertragsstruktur der windata GmbH & Co. KG eingebunden und wird jedem Kunden zur Verfügung gestellt.

Im Bereich der Dienstleister wurden alle notwendigen Auftragsverarbeitungsverträge abgeschlossen.

### 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.*

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

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

PRW hat aufgrund dieser laufenden Rechtskonkretisierungen das Verarbeitungsverzeichnis 2.0 eingeführt, das in folgenden Punkten Veränderungen mit sich bringt:

- Konkretisierung zu den Betroffenenrechten;
- Konkretisierung zur DSFA;
- Konkretisierung bei der Herkunft der Daten;
- Konkretisierung bei den implementierten Maßnahmen;
- Konkretisierung bei den TOM;
- Konkretisierung zu den Transparenzpflichten.

## Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO

*Art. 30 Abs. 2 Satz 1 DSGVO: 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 nicht nur jeden Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO (hierzu zählen Behörden, Unternehmen, Freiberufler, Vereine), sondern auch Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, ein Verzeichnis von Verarbeitungstätigkeiten, welche sie im Auftrag durchführen, zu erstellen und zu führen. Die Regelung des Art. 30 DSGVO bezieht sich dabei jeweils auch auf den Vertreter im Sinne von Art. 4 Nr. 17 DSGVO. Neben der Umsetzung der Verpflichtung nach Art. 30 DSGVO kann das Verzeichnis als Grundlage zur Erfüllung weiterer datenschutzrechtlicher Pflichten verwendet werden.

Wenn ein Unternehmen einzelne Datenverarbeitungsprozesse oder auch seine gesamte Datenverarbeitung im Wege der Auftragsverarbeitung nach Art. 28 DSGVO auf einen Dienstleister überträgt, ist zu klären, wer für welchen Teil der Dokumentation der Verarbeitung zuständig ist.

Art. 30 Abs. 2 DSGVO enthält eine eigene Vorschrift in Bezug auf die Verpflichtung des Auftragsverarbeiters zur Führung eines VVZ.

Darin wird der Auftragsverarbeiter verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. In Abs. 2 a) - d) ist aufgeführt, welche Inhalte dieses Verzeichnis aufweisen muss. Nach Art. 30 Abs. 4 DSGVO muss der Auftragsverarbeiter das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung stellen.

## 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 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.

## 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.*

Aufgrund konkretisierter Best-Practise-Ansätze und Abfragen nach dem Vorhandensein eines Löschkonzepts seitens der Aufsichtsbehörden, ist die Erstellung eines detaillierten Löschkonzepts dringend anzuraten. 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.

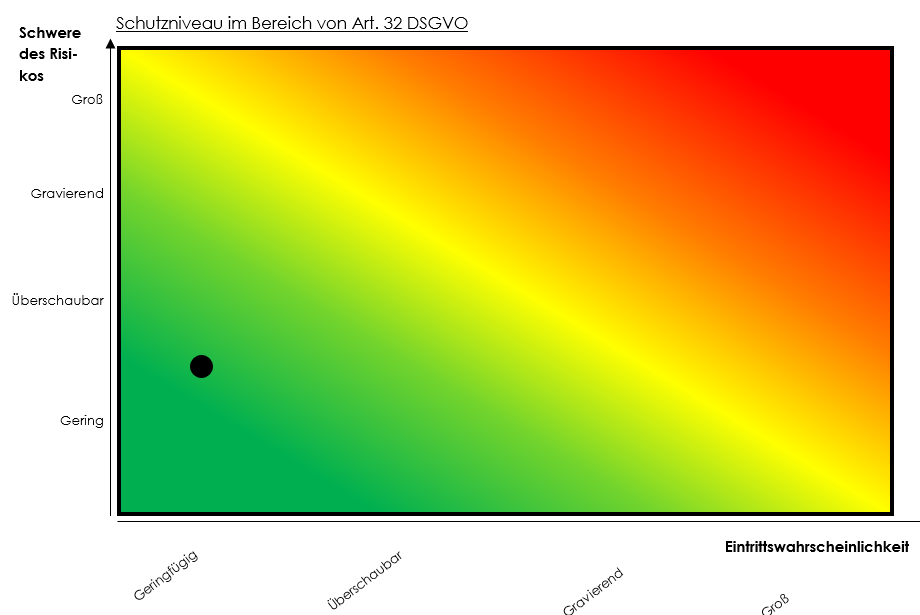
## 7. Technische und Organisatorische Maßnahmen (TOM) - Art. 32 DSGVO -

*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 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 „Standes der Technik“ von 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 Standes der Technik ein angemessenes Schutzniveau gewährleistet wird.

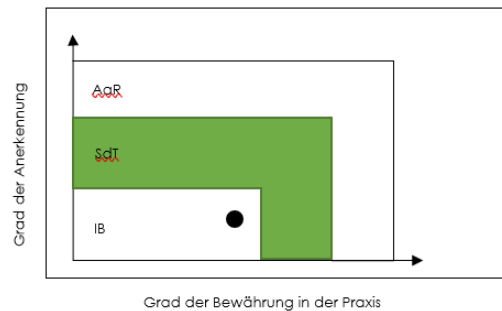
Ausgangspunkt bei der Bewertung der erforderlichen TOM muss immer eine Risikoanalyse bzw. die Betrachtung des erforderlichen Schutzniveaus sein (siehe **Bild 1**) sowie die Betrachtung des Standes der Technik im Bereich der implementierten Maßnahmen (siehe **Bild 2**).



(Bild 1 Bewertung des Schutzniveaus)

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

**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). Insofern empfehlen wir eine erneute Prüfung und Dokumentation der TOM unter den zuvor genannten Aspekten.

Die TOM sollen im Jahr 2022 nochmals geprüft 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.

- Eine Sensibilisierung der Mitarbeiter in den Datenschutzschulungen zum Verhalten bei einer vermeintlichen Datenschutzverletzung ist in Planung.
- Mit den Verantwortlichen werden die notwendigen Vorgehensweisen innerhalb von Schulungs- und Sensibilisierungsmaßnahmen besprochen.

Dem Datenschutzbeauftragten wurde seitens der windata GmbH & Co. KG im Jahr 2021 **keine** Datenschutzverletzung gemeldet.

## 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 Drittlän-der - 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-de-rungen 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).

**Hinweis:** siehe auch C. Ausblick auf 2021, 2. Schrems II

## 10. Website-Check

Aufgrund der neuesten Urteile des Gerichtshofs der Europäischen Union (EuGH) und der entsprechenden Kommentierungen der Aufsichtsbehörde hat der Datenschutzbeauftragte empfohlen, eine Prüfung der Cookies durchzuführen. Dabei ist darauf zu achten, dass alle Cookies erfasst werden, die nicht für den fehlerfreien Gebrauch der Website benötigt werden. Für diese Cookies wird eine wirksame Einwilligung benötigt. Außerdem muss sichergestellt werden, dass die jeweiligen Cookies erst gesetzt werden, nachdem die Einwilligung erfolgt ist.

Zur Sicherheit und um eventuellen Hacker- oder anderen „Angriffen“ vorzubeugen, sollte die Website jederzeit auf dem neuesten Stand sein.

## 11. Fazit zu 2021

Die Anforderungen der DSGVO und des BDSG sind generell bei der windata GmbH & Co. KG 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 windata GmbH & Co. KG. 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 2022**

### **1. Zusammenarbeit**

Die im Rubrum aufgeführten Parteien haben die weitere Zusammenarbeit, auch für den Berichtszeitraum 2022, beschlossen.

### **2. Gesetzliche Neuerungen**

#### **a) Geschäftsgeheimnis**

Mit dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) wurde die EU-Richtlinie ABI EU L 157/1 mit Geltung ab 26.04.2019 in nationales Recht umgesetzt. Dieses Gesetz dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung. Allerdings muss sich ein Unternehmen nach neuer Rechtslage den Geheimnisschutz jetzt aktiv erarbeiten. Nur wenn Geschäftsgeheimnisse definiert, dokumentiert und sodann angemessene Schutzmaßnahmen implementiert wurden, kann ein Unternehmen Ansprüche aus Verletzungen von Geschäftsgeheimnissen geltend machen. Ein entsprechendes dokumentiertes Konzept von technischen, organisatorischen und rechtlichen Maßnahmen ist hierfür erforderlich. Da wir die TOM im nächsten Jahr ohnehin im Fokus haben, könnte hier für Sie eine Kooperation mit PRW Rechtsanwälte interessant sein.

#### **b) Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)**

Das Bundesministerium für Wirtschaft und Energie (BMWi) plant die Schaffung eines Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG). Das geplante Gesetz dient der Umsetzung der ePrivacy-Richtlinie (2002/58/EG) in der Fassung der Richtlinie 2009/136/EG („Cookie“-Richtlinie). Das Gesetz soll für Rechtsklarheit sorgen, da es durch das Nebeneinander von DSGVO, Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) zu Rechtsunsicherheiten kam. Das neue TTDSG soll die Bestimmungen enthalten, die bisher in den §§ 88-107 TKG zur Umsetzung der ePrivacy-Richtlinie (2002/58/EG) enthalten waren sowie weitere Bestimmungen, die bisher dort geregelt sind und die nicht durch die DSGVO ersetzt wurden. Des Weiteren werden die TMG-Datenschutzregelungen, soweit diese durch die DSGVO unberührt geblieben sind, im neuen TTDSG geregelt. Die TMG-Datenschutzregelungen sollen aufgehoben werden.

Ebenso soll eine Rechtsgrundlage für die Anerkennung und Tätigkeit von Diensten zur Verwaltung persönlicher Informationen (Personal Information Management Services - PIMS) als Ansatz einer „Datentreuhand“ geschaffen werden.

Zudem soll die in Deutschland umstrittene Frage zum Setzen von „Cookies“ geklärt werden.

§ 27 TTDS-E ordnet die bisherige geteilte Aufgabenwahrnehmung zwischen Bundesnetzagentur (BNetzA), Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) und den Datenschutzaufsichtsbehörden der Länder neu. Der Bereich des Internetdatenschutzes soll künftig in Deutschland beim BfDI zentralisiert werden.

Das TTDSG soll eine Anpassung an die EU-Richtlinie sein und das Gap bis zur ePrivacy-Verordnung schließen. Ob es die Rechtsunsicherheiten löst oder diese eher verstärkt, das wird sich erst in der Zukunft zeigen. Laut dem Entwurf des TTDSG sollen „funktionierende Geschäftsmodelle weder beeinträchtigt noch Innovationen in der digitalen Welt behindert werden.“

Natürlich respektieren wir unsere Gesetzgebung. Wir würden uns aber manchmal auch etwas mehr die Gelassenheit anderer EU-Staaten im Umgang mit Gesetzen wünschen.

### c) Whistleblowing

Ein Whistleblower (im deutschen Sprachraum zunehmend auch Hinweisgeber, Enthüller oder Aufdecker genannt) ist eine Person, die für die Allgemeinheit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang an die Öffentlichkeit bringt. Dazu gehören typischerweise Missstände oder Verbrechen wie Korruption, Insiderhandel, Menschenrechtsverletzungen, Datenmissbrauch oder allgemeine Gefahren, von denen der Whistleblower an seinem Arbeitsplatz oder in anderen Zusammenhängen erfährt. Bekanntheit hat das Whistleblowing vor allem durch Edward Snowden erlangt.

Am 16.12.2019 ist die EU-Whistleblower-Richtlinie in Kraft getreten (Richtlinie (EU) 2019/1937). Sie verpflichtet die EU-Mitgliedstaaten, die darin enthaltenen Vorgaben binnen zwei (2) Jahren in nationales Recht umzusetzen. Die Frist läuft für den deutschen Gesetzgeber somit am 17.12.2021 ab.

Aber **VORSICHT:** Dann gibt es keine Übergangsfrist mehr. Für viele unserer Mandanten wird die Einführung einer Hinweisgeberstelle also ab dem 17.12.2021 Pflicht sein. Die betroffenen Unternehmen sollten sich schon heute darauf vorbereiten. Daher an dieser Stelle schon einmal die wichtigsten Themen zur Vorbereitung:

- Die Pflicht zur Einführung von Hinweisgebersystemen trifft Unternehmen des Finanzdienstleistungssektors, solche mit fünfzig (50) oder mehr Beschäftigten bzw. solche mit mehr als zehn (10) Millionen Euro Umsatz.
- Die Hinweisgeberstelle soll zur Entgegennahme von Meldungen von Verstößen gegen Unionsrecht eingerichtet werden.



Da aber große Bereiche des nationalen Rechts durch EU-Vorgaben beeinflusst werden, deckt die Whistleblower-Richtlinie maßgebliche rechtliche Bereiche wie Datenschutz, Geldwäsche, Lebensmittel- und Produktsicherheit, die öffentliche Gesundheit, die Umwelt und den Schutz der finanziellen Interessen auch für Deutschland ab.

- Hinweisgeber (also der / die Hinweisgeber) sollen vor negativen Folgen des Whistleblowings jedweder Art geschützt werden. Dies betrifft arbeitsrechtliche Maßnahmen wie Kündigung, Versetzung oder Lohnminderung, ebenso wie sonstige Repressalien.
- **WICHTIG:** Hinweisgeber müssen grundsätzlich Missstände zunächst unternehmensinternen Stellen melden, bevor sie externe Stellen (z. B. Behörden oder die Presse) informieren. Andernfalls genießen sie keinen arbeitsrechtlichen Schutz.
- Da das Whistleblowing sich mit hoher Wahrscheinlichkeit mit (kritischen) personenbezogenen Daten befassen wird (wer macht was?), ist die Erstellung eines VVZ und einer DSFA erforderlich. Wir kommen auf Sie zu, wenn hierzu konkrete Entscheidungen getroffen werden müssen.

München, 12. August 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 2021 PRW Consulting GmbH