O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

Inhaltsverzeichnis

Änderungshistorie

Datum	Version	Erstellt durch	Freigegeben durch	Beschreibung der Änderung
01.05.2018	1	Tom Janzen		neu
01.09.2019	2	Tom Janzen		Korrektur DSB
26.02.2024	3	Tom Janzen		Veröffentlichung Homepage

O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

Präambel

Die Datenschutz-Grundverordnung (DS-GVO) ist am 25. Mai 2016 in Kraft getreten und ist ab dem 25. Mai 2018 wirksam. Sie gilt unmittelbar für alle Mitgliedstaaten der EU, ohne dass sie in das nationale Recht umgesetzt werden muss. Lediglich in einigen Bereichen geben sogenannte „Öffnungsklauseln“ den Mitgliedstaaten die Möglichkeit, bestimmte Themen konkreter zu regeln. Davon hat der deutsche Gesetzgeber Gebrauch gemacht und das sogenannte Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG) beschlossen und damit das Bundesdatenschutzgesetz (BDSG) an die DS-GVO angepasst. Zusätzlich zu der DS-GVO gilt in Deutschland somit das BDSG-neu.

Ziel der europaweiten Regelung ist es zum einen den Datenschutz europaweit zu vereinheitlichen. Bisher galten nationale Datenschutzgesetze in den einzelnen Ländern, die sich erheblich voneinander unterscheiden. Zum anderen sollen auch Betroffenenrechte gestärkt werden.

1. Zweck und Selbstbild

Die Gesetze und Bestimmungen zum Datenschutz und Datensicherheit haben zum Ziel, das Verarbeiten von personenbezogenen Daten nur dann zu erlauben, wenn hierfür ein begründeter und legitimer Zweck gegeben ist. Wenn Daten von Mitarbeitern, Kunden, Lieferanten oder anderen Personen innerhalb des Unternehmens gesammelt, verarbeitet (z.B. auch übermittelt) oder benutzt werden, muss hierbei von allen Beteiligten ein adäquates Datenschutzniveau gewährleistet werden.

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Datenschutzkonzepte und detaillierter Regelungen sowie Arbeitsanweisungen zum Datenschutz und zur Datensicherheit. Diese Leitlinie sowie alle mit dem Datenschutz-Managementsystem verbundenen Dokumente und Prozesse müssen den gesetzlichen Anforderungen entsprechen.

Die Unternehmensleitung betrachtet die informationelle Selbstbestimmung und den Schutz der Daten als hohes Gut – sowohl in Hinsicht auf die Mitarbeiter, wie auch in Bezug auf andere Betroffene (Kunden, Geschäftspartner etc.).

2. Zielvorgaben

Datenschutz-Compliance ist gegenüber Kunden und Mitarbeitern ein Qualitätsmerkmal. Das Unternehmen möchte den Verpflichtungen aus den rechtlichen Vorgaben zum Datenschutz (DS-GVO und nationale Normen) nachkommen und sorgt für ihre Durchsetzung. Dazu hat sich das Unternehmen folgende Ziele gesetzt:

- Einhaltung datenschutzrechtlicher Anforderungen, insbesondere Erfüllung der Anforderungen nach der DS-GVO
- Sicherstellung des Kundenvertrauens durch eine datenschutzgerechte Verarbeitung ihrer Daten
- Minimierung der Risiken und Schäden, denen betroffene Personen ausgesetzt sein könnten

O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

- Hohe Verlässlichkeit der Datenverarbeitung, besonders hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie bei der raschen Wiederherstellung der Verfügbarkeit
- Sicherstellung geeigneter technischer und organisatorischer Maßnahmen inklusive Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen.
- Wahrung der Reputation in der Öffentlichkeit

Diese Ziele leiten sich ebenfalls aus den Geschäftszielen und der Unternehmensstrategie ab und stimmen mit diesen überein.

Die Unternehmensleitung ist für die Überprüfung der Ziele und Zielvorgaben zuständig. Sie bewertet die Erreichung der Zielvorgaben.

3. Chancen

Durch die Etablierung eines Datenschutz-Managementsystems werden personenbezogene Daten, Prozesse und Systeme identifiziert, begutachtet und Verantwortlichkeiten erkannt. Durch eine ausführliche Dokumentation werden zudem die Rechenschafts- und Nachweispflichten erfüllt. Die ständige Überprüfung und kontinuierliche Verbesserung innerhalb des Datenschutz-Managementsystems ermöglicht es, neuen Risiken zu begegnen, neue Anforderungen zu identifizieren und zu erfüllen und damit die Qualität der Systems zu erhöhen. Dadurch werden nicht nur die gesetzlichen Vorgaben erfüllt, sondern dem Unternehmen auch die Chance gegeben, ihre Prozesse zu steuern und zu optimieren.

4. Geltungsbereich

Die Leitlinie stellt ein Dokument auf der obersten Ebene dar. In diesem werden die Ziele, Ausrichtung und Verantwortlichkeiten festgehalten.
Diese Leitlinie erstreckt sich auf das Datenschutz-Managementsystem und gilt für das gesamte Unternehmen.

Die Unternehmensleitung erwartet, dass alle Mitarbeiter, externe Parteien und auch die Unternehmensleitung selbst diese Leitlinie und alle dazugehörigen Regeln, Verhaltensanforderungen und Dokumente beachten und einhalten.

5. Grundbegriffe

Datenschutz: Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch seiner personenbezogenen Daten. Dabei soll das Recht auf informationelle Selbstbestimmung gewährt bleiben, wodurch jeder Mensch nach dem Grundgesetze (GG) der Bundesrepublik Deutschland frei und selbst darüber entscheiden kann, wie mit seinen persönlichen Daten umgegangen wird, sofern kein Gesetz eine andere Regelung vorsieht. Der Einzelne soll wissen, wer, was, wann, bei welcher Gelegenheit über ihn weiß!

O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

Datensicherheit: Unter Datensicherheit wird der Schutz von personenbezogenen Daten vor Verlust, Manipulation, Beschädigung oder Löschung verstanden. Die Datensicherheit soll die Vertraulichkeit, Integrität und Verfügbarkeit von Daten aufrechterhalten.

Personenbezogene Daten: sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Datenschutz-Managementsystem (DSMS): Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, der Implementierung, dem Betrieb und der Überprüfung und Verbesserung des Datenschutzes und der Datensicherheit sicherzustellen

Weitere Definitionen finden sich in der „Datenschutz-Richtlinie“.

6. Maßnahmen zum Datenschutz und damit verbundener Datensicherheit

Der Datenschutz wird in alle Prozesse und Projekte des Unternehmens, bei denen personenbezogene Daten verarbeitet werden, berücksichtigt. Datenschutzanforderungen werden nicht nur bei der Beschaffung von IT, sondern auch bei der Gestaltung von Prozessen sowie bei der Aus- und Weiterbildung von Mitarbeiterinnen und Mitarbeitern mitberücksichtigt.

Es gelten weitere Richtlinien, policies, Datenschutzkonzepte sowie detaillierte Regelungen und Arbeitsanweisungen, um den Datenschutz im Unternehmen zu fördern. In Abwägung des Schutzbedarfes der zu schützenden personenbezogenen Daten, der Risiken sowie des Aufwands werden im Unternehmen angemessene technische und organisatorische Maßnahmen identifiziert und implementiert.

7. Verantwortlichkeiten für den Datenschutz

Grundsätzlich bestehen die folgenden Verantwortlichkeiten:

Unternehmensleitung
Der Unternehmensleitung obliegt die Gesamtverantwortung für den Datenschutz. Diese steht daher in vollem Umfang hinter den in dieser Leitlinie formulierten Zielen und den daraus abgeleiteten Konzepten und Maßnahmen.

Sie ist dafür verantwortlich, dass Datenschutz und Datensicherheit umgesetzt und kontinuierlich verbessert wird. Hierfür stellt die Unternehmensleitung die erforderlichen Ressourcen zur Verfügung.

O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

Die Unternehmensleitung ist insbesondere verantwortlich für:

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Datenschutz und Datensicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Datenschutz-Managementsystems,
- die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen einschließlich der Bereitstellung der erforderlichen Ressourccen,
- eine hinreichende und geeignete Dokumentation, um nachweisen zu können, dass das Unternehmen Datenschutz und Datensicherheit entsprechend der DS-GVO umgesetzt hat
- die Einbettung des Datenschutzes und der Datensicherheit in die Strukturen, Hierarchien und Arbeitsabläufe des Unternehmens.

Datenschutzbeauftragter (DSB)
Der DSB überwacht die Einhaltung des Datenschutzes und der Datensicherheit und ist für die Koordination des Betriebes des DSMS zuständig. Seine Pflichten sind insbesondere in Art. 39 DSGVO geregelt. Weiterhin bestehen die folgenden Aufgabenbereiche:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den geltenden Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- Anlaufstelle für und Zusammenarbeit mit der Aufsichtsbehörde
- Weitere Aufgaben sind an den DSB delegierbar, sofern hierdurch keine Interessenkonflikte entstehen

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.

Verantwortung des Einzelnen inkl. der Unternehmensleitung
Alle Mitarbeiter gewährleisten den Datenschutz und die Datensicherheit durch verantwortungsbewusstes Handeln und halten die hierfür relevanten Gesetze, Vorschriften, Richtlinien und Anweisungen sowie vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten personenbezogenen Daten, Informationen und IT-Systemen um.

Verhalten, das die Sicherheit von personenbezogene Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden und unter Umständen können zivilrechtliche Ansprüche geltend gemacht werden.

O.V.-Ostfriesische Versicherungsbörse Assekuranzen GmbH

Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der personenbezogenen Daten Ist von jedem Mitarbeiter in seinem Aufgabenbereich zu beachten.

Jeder Beschäftigte sowie externe Parteien melden dem DSB bzw. der Geschäftsleitung alle Datenschutzvorfälle bzw. Sicherheitslücken.

Verantwortung externer Parteien (Leistungserbringer)
Personen, Unternehmen und öffentliche Hand, die nicht zum Unternehmen gehören, für diese aber Leistungen erbringen, haben die Vorgaben des Unternehmens zur Einhaltung des Datenschutzes und der Datensicherheit gemäß dieser Leitlinie einzuhalten. Das Unternehmen informiert die externe Partei über diese Regeln und verpflichtet sie in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass die externe Partei bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen das Unternehmen zu informieren hat.

8. Kommunikation

Die Unternehmensleitung stellt sicher, dass die Leitlinie allen Mitarbeitern sowie externen Parteien bekannt ist und beachtet wird.

9. Unterstützung durch die Unternehmensleitung und Selbstverpflichtung

Die Einhaltung eines angemessenen Datenschutzniveaus erfordert finanzielle, personelle und zeitliche Ressourcen. Die Unternehmensleitung erklärt, dass sie die Implementierung des Datenschutz-Managementsystems (DSMS) sowie die kontinuierliche Verbesserung mit geeigneten Ressourcen unterstützen wird, damit die gesetzten Ziele sowie gesetzlichen Datenschutzanforderungen erfüllt werden.

Unterschrift Unternehmensleitung