Datenschutz- und Datensicherheitsleitlinie der Andre Reinisch Barnim Finanz UG(haftungsbeschränkt)&Co.KG

Verantwortliche Stelle
Andre Reinisch Barnim Finanz UG(haftungsbeschränkt) & Co.KG
Rudolf-Breitscheid-Strasse 2
16225 Eberswalde
Vertreten durch
Andre Reinisch
(Geschäftsführer)

Präambel

Grundwerte der Andre Reinisch Barnim Finanz UG (haftungsbeschränkt) & Co.KG
(weiterhin Firma genannt)

Unsere oberste Priorität ist die messbare Zufriedenheit unserer Kunden. Denn nur wenn der Kunde mit unseren Leistungen zufrieden ist, können wir ihn langfristig an unser Unternehmen binden und begeistern. Wir sichern mit unserem ganzen Engagement und unserer Kompetenz die individuellen Risiken unserer Kunden ab und wachsen im gemeinsamen Austausch mit den sich ständig verändernden Risiken.
Unsere Lösungen sind von Beginn an die aus unserer Sicht für den Kunden besten Lösungen am Markt, die fortwährend im Sinne des Best-Advice an die Bedürfnisse und Lebenssituationen unserer Kunden angepasst werden.

Prinzipien

Die Firma handelt verantwortungsbewusst gegenüber ihren Kunden, Geschäftspartnern und deren Mitarbeitern. Wir verpflichten uns zur Einhaltung ethischer Grundsätze und Verhaltensregeln. Wir pflegen eine offene und vertrauensvolle Kommunikation. Diese Prinzipien sind die Grundlage für die Zufriedenheit unserer Mitarbeiter und Kunden.

Dabei ist davon auszugehen, dass auch personenbezogene und besondere personenbezogene Daten erhoben, verarbeitet und genutzt werden müssen.

Grundlagen
Gemäß §46 Absatz 1 des Bundesdatenschutzgesetzes BDSG(neu) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen

Aus dem allgemeinen Persönlichkeitsrecht Art. 1 Abs. 1 Grundgesetz ergibt sich ein Recht auf informationelle Selbstbestimmung. Der Datenschutz bezweckt somit den Schutz des Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch den angemessenen Umgang mit seinen personenbezogenen Daten.

In Deutschland ist der Umgang mit personenbezogenen Daten in Umsetzung völkerrechtlicher und europäischer Verpflichtungen neben dem Bundesdatenschutzgesetz durch die Datenschutzgesetze der Länder und Spezialgesetze, wie zum Beispiel das Telekommunikationsgesetz und das Telemediengesetz festgeschrieben.

Die Firma unterfällt dem DSGVO und dem BDSG(neu). Damit obliegt es ihr, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der DSGVO zu gewährleisten.

Ziele

Mit dieser Leitlinie zum Datenschutz und zur IT-Sicherheit gibt sich die Firma den Rahmen für den Umgang mit personenbezogenen Daten und den sicheren Betrieb der informationstechnischen Infrastrukturen und Organisationsstrukturen, die für die Erbringung der Dienstleistungen der Firma benötigt werden.

Selbstverpflichtung und Leitbild

Der Datenschutz, der sichere und vertrauensvolle Umgang mit Daten und die verantwortungsvolle Nutzung der informationstechnischen Infrastruktur ist besonderes Anliegen der Geschäftsführung.

Die Geschäftsführung und die Mitarbeiter der Firma sind sich ihrer Verantwortung bei der Erbringung der Dienstleistungen und im Umgang mit den dafür eingesetzten informationstechnischen Infrastrukturen bewusst und beachten die einschlägigen Gesetze und vertraglichen Regelungen.

Die Umsetzung von Datenschutz und IT-Sicherheit hat einen hohen Stellenwert. Alle notwendigen, geeigneten und angemessenen Maßnahmen werden getroffen, um negative materielle und immaterielle Folgen für Betroffene und die Firma auszuschließen.

Als Vertreter der Interessen von Kunden und Mandanten fühlt sich die Firma verpflichtet, ergänzend zur Umsetzung des Datenschutzes und der IT-Sicherheit in seinen eigenen Arbeitsabläufen deren Interessen zu wahren und für einen verantwortungsvollen Umgang der anfallenden persönlichen Daten einzustehen.

Leitsätze

Die Firma schützt die personenbezogenen oder sonstigen vertraulich zu behandelnden Daten ihrer Mandanten, ihrer Kundinnen und Kunden, Produktgeber sowie ihrer Beschäftigten und Mitarbeiter.
Schutzbedarf besteht nicht nur für personenbezogene Daten, sondern auch für sonstige vertrauliche Informationen, wie z. B. Finanz- oder Planungsdaten.

Die Verarbeitung personenbezogener Daten ist ohne gesetzliche Grundlage oder ohne Einwilligung des Betroffenen verboten.
Es werden nur die Daten verarbeitet, die für die rechtmäßige Aufgabenerfüllung erforderlich sind. Die Daten werden nur für Zwecke verarbeitet, für die sie erhoben worden sind.

Die Gewährleistung von Datenschutz und Datensicherheit ist Aufgabe und Verpflichtung für alle Beschäftigten.
Die Mitarbeiter/innen sind als Nutzer von IT-Systemen bei der Verarbeitung von Daten verpflichtet, diese Leitlinie und die daraus abgeleiteten Standards und Richtlinien – insb. der IT-Sicherheitsrichtlinie - zu beachten.

Die Führungskräfte sind für die Einhaltung eines angemessenen Sicherheitsstandards im Datenschutz und in der Datensicherheit verantwortlich.
Alle Führungskräfte sind dafür verantwortlich, die bestehenden Sicherheitsstandards in ihrem Fach bzw. Geschäftsbereich umzusetzen und aufrecht zu erhalten. Hierfür sind die organisatorischen, personellen und technischen Voraussetzungen zu realisieren.

Prinzipien
Der Umgang mit personenbezogenen Daten ist im bundesdeutschen Datenschutzrecht und in der DSGVO als Verbot mit Erlaubnisvorbehalt geregelt. Damit ist das Erheben, Verarbeiten, Übermitteln und Nutzen von personenbezogenen Daten grundsätzlich verboten. Eine Ausnahme ergibt
Sich nur, wenn ein Gesetz oder eine andere Rechtsverordnung dies erlaubt oder der Betroffene einwilligt.

Prinzip der Datenvermeidung
Hieraus leitet die Firma ab, für alle seine Arbeitsvorgänge die Erhebung, Verarbeitung, Übermittlung und Nutzung von personenbezogenen Daten soweit möglich zu vermeiden.

Prinzip der Erforderlichkeit
Soweit bei Arbeitsvorgängen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nicht vermieden werden kann, wählt die Firma im Rahmen des technisch Vertretbaren jeweils den Arbeitsvorgang, bei dem so wenig personenbezogene Daten wie möglich erhoben, verarbeitet, übermittelt und genutzt werden müssen.

Prinzip der Zweckbindung
Eine Verwendung von personenbezogenen Daten für einen anderen als den vorab festgelegten Zweck ist ausgeschlossen, es sei denn es liegt eine Einwilligung des Betroffenen vor oder ein Gesetz bzw. eine Rechtsvorschrift erlaubt oder ordnet dies an.

Prinzip der Datensparsamkeit
Bei allen Arbeitsvorgängen werden die gesetzlichen Löschfristen beachtet. Werden personenbezogene Daten nicht mehr benötigt, werden sie ohne Ausschöpfung der Löschfristen vorzeitig gelöscht.

IT-Sicherheit
Eine wirksame Umsetzung des Datenschutzes ist nur mit einer wirkungsvollen IT-Sicherheit zu erreichen. Entsprechend formuliert die Firma neben den Prinzipien
zur Umsetzung des Datenschutzes Prinzipien zur IT-Sicherheit und eine daraus resultierende IT-Sicherheitsrichtlinie

Die Vermeidung von Unterbrechungen und Inkonsistenzen der datenverarbeitenden Dienste spielt für die Ansprüche an den Datenschutz der Firma eine maßgebliche Rolle bei der Ausübung der Betroffenenrechte. Deswegen werden die für die Erbringung von Dienstleistungen eingesetzten informationstechnischen Infrastrukturen in ihrer Verfügbarkeit und Fehlerfreiheit bereitgestellt und gesichert.

Fehlfunktionen und Unregelmäßigkeiten in Daten und informationstechnischen Infrastrukturen sind nur in sehr geringem Umfang und nur in Ausnahmefällen akzeptabel.
Daher werden die Daten und informationstechnischen Infrastrukturen der Firma in ihrer Integrität gesichert.

Die unberechtigte Einsichtnahme oder Weitergabe von Daten der Firma ist nicht zulässig. Um den Anforderungen an den Schutz sensibler Daten zu entsprechen, werden die Daten und informationstechnischen Infrastrukturen in ihrer Vertraulichkeit gesichert und alle Mitarbeiter in ihrer Nutzung und Funktion eingewiesen und geschult.

Umsetzung

Die Umsetzung des Datenschutzes und der IT-Sicherheit in den Arbeitsabläufen der Firma erfordert technische und organisatorische Maßnahmen. Diese Maßnahmen werden in weiterführenden Dokumenten festgelegt und laufend aktuell gehalten.
Zur Abwehr und zur Minderung der Folgen von Angriffsversuchen auf die informationstechnischen Infrastrukturen ergreift die Firma sowohl proaktive als auch zeitnahe reaktive Maßnahmen.

Geltungsbereich

Diese Leitlinie gilt für die Firma, deren Mitarbeiter, den externen Dienstleistern und Lieferanten.

Geltungsdauer

Diese Leitlinie tritt mit dem 25.05.2018 in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.