

VERTRAULICHKEITS- UND VERSCHWIEGENHEITS- VEREINBARUNG (NDA)

zwischen
items GmbH & Co.KG
Hafenweg 7
48151 Münster

- nachfolgend bezeichnet als "**Informationsinhaber/Auftraggeber**" -

und

Daten Auftragnehmer

- nachfolgend bezeichnet als "**Informationsempfänger/Auftragnehmer**" -

- beide nachfolgend als "die **Vertragsparteien**" bezeichnet –

Alle Begrifflichkeiten verstehen sich geschlechtsneutral.

wird die folgende Vereinbarung geschlossen:

PRÄAMBEL

Die folgende Vertraulichkeitsvereinbarung (nachfolgend „Vereinbarung“) wird vor dem Hintergrund der Geschäftsbeziehung zwischen dem Informationsempfänger und dem Informationsinhaber geschlossen. Der Informationsinhaber ist gesetzlich verpflichtet und hat ein geschäftliches Interesse daran, vertrauliche Informationen und insbesondere Geschäftsgeheimnisse sowie personenbezogene Daten zu schützen, die der Informationsempfänger im Rahmen der Geschäftsbeziehung zur Kenntnis nehmen kann.

Mit der Vereinbarung werden daher Vertraulichkeitspflichten festgelegt, die den Vertragsparteien als Basis für eine rechtssichere und vertrauensvolle Zusammenarbeit dienen sollen. Welche Informationen als vertraulich gelten, bestimmt sich entsprechend der Anlage zu dieser Vereinbarung. Der Informationsinhaber bittet, die Vereinbarung sorgfältig zu lesen und steht bei Fragen die Vereinbarung betreffend zur Verfügung.

BEGRIFFLICHKEITEN UND DEFINITIONEN

- a) "Geschäftsbeziehung" - Der Begriff der Geschäftsbeziehung umfasst alle Arten laufender Geschäftsbeziehungen zwischen dem Informationsinhaber und dem Informationsempfänger, in deren Rahmen der Informationsempfänger vertrauliche Informationen des Informationsinhabers zur Kenntnis nehmen kann. Sofern die Geltung dieser Vereinbarung anderweitig (d. h. innerhalb dieser Vereinbarung oder außerhalb, in anderen Verträgen oder Regelungen) auf bestimmte Arten, Typen oder konkrete Geschäftsbeziehung, Verträge, etc. beschränkt wurde, sind diese jeweils als Geschäftsbeziehung zu verstehen.
- b) "Vertrauliche Informationen" - Als vertrauliche Informationen im Sinne dieser Vereinbarung sind unabhängig von ihrer Bezeichnung sowie ihrer Verkörperung oder Mitteilungsart (z. B. Papierform, digital, mündlich) Informationen zu verstehen, über die der Informationsinhaber zum einen die Kontrolle hat, die Unbefugten nicht in Gänze oder Teilen rechtmäßig zugänglich sind (insbesondere Geschäftsgeheimnisse) oder zu deren Schutz der Informationsinhaber selbst verpflichtet ist (insbesondere personenbezogene Daten). Als vertraulich sind insbesondere Informationen anzusehen, die von dem Informationsinhaber als vertraulich gekennzeichnet oder als vom Gesetz als vertraulich oder vor unerlaubtem Zugriff durch Dritte zu schützend bestimmt werden.
- c) "Geschäftsgeheimnis" - Als Geschäftsgeheimnisse im Sinne dieser Vereinbarung sind Informationen zu verstehen, die weder öffentlich noch Unbefugten zugänglich sind und daher über einen wirtschaftlichen Wert für den Informationsinhaber verfügen. Dies gilt unabhängig von der Bezeichnung der Informationen (z. B. als Betriebs- oder Fabrikationsgeheimnisse). Ein Geschäftsgeheimnis kann ebenfalls dann vorliegen, wenn es durch den Informationsempfänger im Rahmen seiner Tätigkeit für den Informationsinhaber geschaffen wurde, auch wenn der Informationsinhaber selbst von dem Geschäftsgeheimnis noch keine Kenntnis hat. Ein Geschäftsgeheimnis kann auch die Information sein, dass der Informationsinhaber bestimmte Verfahren, Software oder Dienstleister einsetzt (auch wenn diese selbst öffentlich bekannt sind). Zu den Geschäftsgeheimnissen gehören insbesondere die als solche in Anhang 1 zu dieser Vereinbarung definierten Geschäftsgeheimnisse.
- d) "Personenbezogene Daten" im Sinne des Art. 4 Nr. 1 DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z. B. Mitarbeiter, Kunden, etc.); 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. Personenbezogene Daten dürfen nur entsprechend den gesetzlichen Vorschriften, z. B. auf Grundlage einer Einwilligung oder wenn die Verarbeitung zur Erfüllung von Verträgen erforderlich ist, verarbeitet werden. Die Verarbeitung umfasst auch die Übermittlung oder Offenbarung von personenbezogenen Daten (Art. 4 Nr. 2 DSGVO).
- e) "Dritte" - Als Dritte werden Personen, Unternehmen und sonstige Rechtssubjekte bezeichnet die weder der Informationsinhaber oder der Informationsempfänger oder deren Beschäftigten sind. Zu den Dritten gehören insbesondere Subunternehmer der Informationsempfänger (deren Einsatz erlaubt sein muss).

- f) "Nutzung" - Als Nutzung von Geschäftsgeheimnissen ist jede Art ihrer Verwendung, Anwendung, des Einsatzes, der Inanspruchnahme von Gebrauchsvorteilen, entgeltlich und unentgeltlich, im geschäftlichen sowie im privaten Rahmen, selbst oder durch den Einsatz von Dritten zu verstehen. Im Fall von personenbezogenen Daten ist als Nutzung jede Art der Verarbeitung im Sinne des Art. 4 Nr. 1 DSGVO zu verstehen.
- g) "Offenlegung" - Als Offenlegung ist jede Ermöglichung des Zugangs, der Kenntnisnahme, Übermittlung oder sonstige Eröffnung einer vertraulichen Information zu verstehen.
- h) "Unbefugte" - Als unbefugt, bzw. als Unbefugte gelten Personen, Unternehmen oder sonstige Dritte, denen die vertraulichen Informationen bestimmungsgemäß nicht zugänglich sind, wozu insbesondere auch Mitarbeiter des Informationsempfängers und wirtschaftlich verbundene Unternehmen gehören.

VERTRAULICHKEITS-, SCHUTZ-, UND INFORMATIONSPFLICHTEN

- a) Der Informationsempfänger wird Vertrauliche Informationen, die ihm im Rahmen der Geschäftsbeziehung mit dem Informationsinhaber zur Kenntnis gelangen oder sonst bekannt werden, bzw. in den eigenen Verfügungsbereich gelangen, vertraulich behandeln. Der Informationsempfänger wird die ihm zumutbaren, zum Schutz vertraulicher Informationen erteilte Weisungen und Hinweise des Informationsinhabers beachten. Der Informationsempfänger wird die vertraulichen Informationen nur im Rahmen der Zwecke, zu denen er die vertraulichen Informationen erhalten hat, in dem für diese Zwecke erforderlichen Umfang sorgfältig nutzen, vor Offenlegung gegenüber Unbefugten schützen und nicht für andere Zwecke, auch nicht für eigene private Zwecke, nutzen.
- b) Der Informationsempfänger wird die ihm im Hinblick auf den Schutz der vertraulichen Informationen dem Stand der Technik entsprechende technische und organisatorische Maßnahmen (TOM) und die ihm von dem Informationsinhaber auferlegten TOM (gemäß Anhang 2) implementieren. Der Informationsempfänger wird in jedem Fall dafür sorgen, dass der Zugang zu vertraulichen Informationen innerhalb des eigenen Organisationsbereichs auf das erforderliche Maß beschränkt wird (so genanntes "need to know"-Prinzip). Mitarbeiter müssen über die Pflicht zum Schutz von vertraulichen Informationen unterrichtet und auf dessen Einhaltung verpflichtet werden.
- c) Der Informationsempfänger wird seine Mitarbeiter auf Wahrung der Vertraulichkeit und Verschwiegenheit im Hinblick auf Vertrauliche Informationen und Einhaltung der sich aus dieser Vereinbarung ergebenden Pflichten verpflichten sowie die Einhaltung der Verpflichtung sicherstellen.
- d) Die Nutzungs-, Verwertungs-, Eigentums-, Inhaber- und andere Schutzrechte an den vertraulichen Informationen stehen alleine dem Informationsinhaber zu. Der Informationsempfänger wird es nicht anstreben, für sich oder für Dritte eigene Verwertungsmöglichkeiten und Rechte an den vertraulichen Informationen zu erlangen, z. B. durch Anmeldung von gesetzlichen Schutzrechten, wie Patent-, Design- oder Markenrechten.
- e) Der Informationsempfänger wird Hard- und Software sowie sonstige Produkte, Einrichtungen, Anlagen, zu denen der Informationsempfänger im Rahmen der Geschäftsbeziehung Zugang erhält, ohne hierzu angewiesen oder sonst von dem Informationsinhaber befugt zu sein, in Gänze, in Teilen und unabhängig von der Entwicklungsphase nicht zum Zweck oder mit Folge der Gewinnung von vertraulichen Informationen beobachten, untersuchen, rückbauen oder testen (sogenanntes „Reverse Engineering“).
- f) Wird der Informationsempfänger im Rahmen der Geschäftsbeziehung zum Informationsinhaber innerhalb von Plattformen und Arbeitsumgebungen oder mit Software, die von Drittanbietern angeboten werden (nachfolgend bezeichnet als "Drittumgebungen"), tätig, verpflichtet sich der Informationsempfänger, in diesem Rahmen die Geschäftsbedingungen (z. B. AGB, Nutzungsbedingungen, Datenschutzbedingungen, Richtlinien, oder technische Vorgaben) der Drittumgebungen einzuhalten und nur nach Weisung des Informationsinhabers zu handeln. Der Informationsempfänger verpflichtet sich Daten (insbesondere Vertrauliche Informationen), die er in diesem Rahmen von dem jeweiligen Anbieter der Drittumgebungen erhält oder in diesem Zusammenhang erhebt oder sonst verarbeitet, nur im Rahmen der Geschäftsbeziehung zum Informationsinhaber zu vereinbarten Zwecken zu verarbeiten. Der

Informationsempfänger wird die Daten ohne Zustimmung des Informationsinhabers, keinen dritten Unternehmen oder Personen zur Verfügung zu stellen oder ihnen die Verarbeitung der Daten ermöglichen. Der Informationsempfänger verpflichtet sich im Fall des Einsatzes von Sub-, bzw. Unterauftragnehmern, diese entsprechend den vorgenannten Verpflichtungen im Hinblick auf die Drittumgebungen ebenfalls und nachweislich zu verpflichten. Der Informationsinhaber ist berechtigt, die Beauftragung, bzw. Einsatz des Informationsempfängers und seiner Sub-/ oder Unterauftragnehmer in diesem Rahmen gegenüber den Anbietern der Drittumgebungen offen zu legen.

- g) Sofern der Informationsempfänger die vertraulichen Informationen gegenüber Dritten offenbart und die Dritten dem Informationsinhaber nicht bekannt sind oder bekannt sein müssten, ist der Informationsempfänger in einem zumutbaren Rahmen verpflichtet, dem Informationsinhaber auf Anfrage eine Liste der Dritten und der betroffenen vertraulichen Informationen zu überlassen sowie die Umstände der Offenbarung mitzuteilen.
- h) Der Informationsempfänger wird den Informationsinhaber über mögliche stattgefundene oder drohende Verletzungen des Schutzes von vertraulichen Informationen auch bereits bei begründetem Verdacht unverzüglich informieren (z. B. im Fall des Verlusts von Datenträgern, Fehlversandes von E-Mails oder unerlaubten Zugriffs auf IT-Systeme durch unbefugte Personen). Die Meldepflicht besteht im zumutbaren Rahmen auch, wenn der Informationsempfänger kraft Gesetzes, behördlicher Anordnungen und vergleichbarer zwingender Maßnahmen zur Offenlegung der vertraulichen Informationen gegenüber Dritten verpflichtet wird. In allen vorbenannten Fällen hat der Informationsempfänger alle ihm zumutbaren Maßnahmen zu ergreifen und Anstrengungen zu unternehmen sowie den Informationsinhaber zu unterstützen, um das Maß der Gefährdung oder Offenlegung der vertraulichen Informationen soweit wie möglich zu beschränken.
- i) Falls der Informationsempfänger beabsichtigt, Vertrauliche Informationen offenzulegen und diese Offenlegung dem Informationsinhaber nicht bereits bekannt ist, hat der Informationsempfänger den Informationsinhaber bereits über eine beabsichtigte Offenlegung sowie ihren (Rechts)Grund (z. B. Berufung auf eine Ausnahme vom Schutz als Geschäftsgeheimnis) vorab zu informieren (grundsätzlich in Text- oder Schriftform). Die Vorabinformation muss innerhalb einer angemessenen Vorabfrist erfolgen, die grundsätzlich 14 Werktage beträgt. Eine Pflicht zu Vorabinformation besteht nicht, falls und sofern die Vorabinformation dem Informationsempfänger nicht möglich und nicht zumutbar ist. Der Informationsempfänger wird in diesem Zusammenhang darauf hingewiesen, dass Vorgänge innerhalb der Geschäftsbeziehung grundsätzlich zuerst intern zu klären und an den Informationsinhaber zu melden sind, bevor sie gegenüber Dritten offenbart werden. Ferner hat der Informationsempfänger die gesetzlich zulässigen, möglichen und zumutbaren sowie erforderlichen Vorkehrungen zu treffen, um den Umfang der Offenlegung so gering wie möglich zu halten.
- j) Sofern gesetzlich erforderlich, schließt der Informationsempfänger weitere Vereinbarungen im Hinblick auf den Schutz vertraulicher Informationen mit dem Informationsinhaber oder gibt erforderliche Vertraulichkeits- und Verschwiegenheitszusagen ab (z. B. im Falle der Verarbeitung von personenbezogenen Daten im Auftrag).

BEAUFTRAGUNG VON DRITTEN

- a) Der Einsatz von Subunternehmern oder anderen Dritten bestimmt sich nach den Regelungen der Geschäftsbeziehung.
- b) Der Informationsempfänger darf Subunternehmer oder andere Dritte (nachfolgend zusammen bezeichnet als "Dritte") mit der Wahrnehmung der Vertragspflichten gegenüber dem Informationsinhaber beauftragen, sofern dies mit einem angemessenen zeitlichen Vorlauf, der grundsätzlich 10 Werktage nicht unterschreiten darf, erfolgt. Dem Informationsinhabers steht ein Recht dem Einsatz der Dritten zu widersprechen. Der Informationsempfänger macht von seinem Recht auf Einspruch nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.
- c) Der Informationsempfänger stellt sicher, dass die Dritten zur Einhaltung der im Rahmen dieser Vereinbarung geltenden Pflichten gleichermaßen verpflichtet werden, stellt die Einhaltung dieser Pflichten sicher und weist dies auf Anfrage des Informationsinhabers nach.

- d) Unternehmen oder Personen, deren Leistungen der Informationsempfänger nicht zur Wahrnehmung seiner Pflichten aus der Geschäftsbeziehung, sondern als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z. B. Reinigungs-, Bewachungs- oder Transportleistungen) sind, ebenso wie der Einsatz von Mitarbeitern des Informationsempfängers, nicht als Beauftragung von Dritten im Sinne dieses Abschnitts "Beauftragung von Dritten" dieser Vereinbarung zu verstehen. Gleichwohl hat der Informationsempfänger sicher zu stellen, z. B. durch vertragliche Vereinbarungen, Hinweise und Instruktionen, dass hierbei die Sicherheit der vertraulichen Informationen nicht gefährdet wird und die Vorgaben dieser Vertraulichkeitsvereinbarung sowie die Gesetze eingehalten werden.

VERTRAGSSTRAFENVEREINBARUNG

- a) Der Informationsempfänger verpflichtet sich, für jeden Fall einer schuldhaften Verletzung der in dieser Vereinbarung oder der gesetzlich geregelten Pflichten zum Schutz von vertraulichen Informationen eine Vertragsstrafe an den Informationsinhaber zu zahlen. Die Vertragsstrafe wird entsprechend der Schwere und dem Ausmaß der Verletzung nach Billigkeitsgesichtspunkten in angemessener Höhe durch den Informationsinhaber festgelegt. Die Höhe der Vertragsstrafe sowie deren Angemessenheit, können im Streitfall von dem zuständigen Gericht überprüft werden.
- b) Das Recht des Informationsinhabers zur Geltendmachung eines weitergehenden Schadens sowie etwaiger Rechtsbehelfe und Maßnahmen des einstweiligen Rechtsschutzes bleibt unberührt.

LAUFZEIT UND PFLICHTEN NACH VERTRAGSENDE

- a) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft und endet drei Jahre nach Beendigung der Geschäftsbeziehung bzw. der Offenlegung der vertraulichen Informationen gegenüber dem Informationsempfänger, je nachdem, welches Ereignis später eintritt.
- b) Der Informationsempfänger wird unverzüglich, sofern nicht anders vereinbart, spätestens innerhalb von sieben Werktagen nach Beendigung der Geschäftsbeziehung oder falls die vertraulichen Informationen für die Durchführung der Geschäftsbeziehung nicht mehr erforderlich werden, die erlangten Träger von vertraulichen Informationen und/ oder Zugangsberechtigungen zu vertraulichen Informationen unabhängig von der Art und Form (z. B. Unterlagen und Dateien einschließlich etwaiger Vervielfältigungsstücke, Passwörter, Schlüssel etc.) an den Informationsinhaber zurückzugeben. Die Frist kann aufgrund der Umstände des Einzelfalls verkürzt oder verlängert werden kann, was jedoch die Begründung der Friständerung voraussetzt und sowohl für die andere Vertragspartei auch als mit Rücksicht auf andere Parteien, z. B. datenschutzrechtlich betroffene Personen, angemessen und zumutbar sein muss. Alternativ wird der Informationsempfänger nach Wahl des Informationsinhabers/ oder falls die Rückgabe dem Informationsempfänger nicht möglich oder nicht zumutbar ist (z. B. aufgrund gesetzlicher Aufbewahrungspflichten), die Informationsträger, bzw. die Zugangsberechtigungen nach Rücksprache mit dem Informationsinhaber vernichten, bzw. zu löschen. Die Vernichtung/ Löschung ist so durchzuführen, dass die Wiedergewinnung der vertraulichen Informationen ausgeschlossen ist. Geltende Industrienormen sind zu beachten. Der Informationsempfänger wird die Vernichtung oder Übergabe nach Aufforderung des Informationsinhabers in angemessener Form, zumindest schriftlich, bestätigen. Dem Informationsempfänger steht im Hinblick auf die Vertrauliche Informationen kein Zurückbehaltungsrecht zu.
- c) Die sich aus der Vertraulichkeitsvereinbarung ergebenden Pflichten zum Schutz vertraulicher Informationen gelten auch nach Ende der Geschäftsbeziehung fort, sofern die Informationen weiterhin zu Gunsten des Informationsinhabers als vertraulich gelten und die Beachtung der Vertraulichkeitsverpflichtung nicht zu einer unangemessenen oder unbilligen Einschränkung der wirtschaftlichen oder beruflichen Betätigung des Informationsempfängers führen. Sollte eine derartige Einschränkung zu befürchten sein, werden hierzu zwischen den Vertragsparteien entsprechende Vereinbarungen, insbesondere zu einer angemessenen Karenzzeit, getroffen.

GELTENDES RECHT, GERICHTSSTANDORT UND SCHLUSSBESTIMMUNGEN

- a) Die Rechtsbeziehungen zwischen dem Informationsinhaber und dem Informationsempfänger unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland. Die Vereinbarung des anwendbaren Rechts findet auch dann Anwendung, wenn sich der Sitz des Informationsempfängers und/oder die Wohnanschrift im Ausland befindet.
- b) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist der (Wohn)Sitz des Informationsinhabers und sofern vom geltenden Gesetz zwingend vorgesehen, der Informationsempfänger Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Informationsempfänger im Geltungsbereich des anwendbaren Rechts keinen Gerichtsstand hat. Der Informationsinhaber behält sich vor, Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.
- c) Die vorliegende Vereinbarung stellt die vollständige, zwischen den Vertragsparteien getroffene Vereinbarung dar. Mündliche Nebenabreden bestehen nicht.
- d) Änderungen sowie Ergänzungen dieser Vereinbarung, als auch die Aufhebung dieser Formklausel und die Kündigung der Vereinbarung bedürfen zumindest der elektronischen Form. Damit ist z. B. die auf dauerhaften Datenträgern gespeicherte Vereinbarung per E-Mail, digitale Signiervverfahren oder via dedizierte Onlinefunktionen (z. B. in Benutzerkonten) gemeint. Die elektronische Form setzt die Erkennbarkeit der Person des Erklärenden voraus.
- e) Sollten eine oder mehrere Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die unwirksamen Bestimmungen werden vielmehr im Wege der ergänzenden Auslegung durch eine solche Regelung ersetzt, die von den Vertragsparteien mit der/ den unwirksamen Bestimmung/en erkennbar verfolgten wirtschaftlichen Zweck möglichst nahekommt. Sofern die vorbenannte ergänzende Auslegung aufgrund gesetzlich zwingender Vorgaben nicht möglich ist, werden die Vertragsparteien eine ihr entsprechende Regelung vereinbaren.

.....
Ort, Datum, Unterschrift Informationsempfänger

.....
Ort, Datum, Unterschrift Informationsinhaber

Anhang 1: Von der Vereinbarung umfasste Geschäftsgeheimnisse

Im Folgenden werden die von dieser Vereinbarung umfassten Geschäftsgeheimnisse, als auch die Ausnahmen von dem Schutz als Geschäftsgeheimnis definiert.

Zu den Geschäftsgeheimnissen im Sinne dieser Vereinbarung gehören insbesondere die folgenden Informationen:

- Der Inhalt dieser und anderer Vereinbarungen.
- Informationen zu Vergütungs- und sonstige Zahlungsvereinbarungen zwischen dem Informationsinhaber und Informationsempfänger, deren Durchführung, Zahlende und Zahlungsempfänger sowie Höhen von Entgelten.
- Angaben zu Absatz, Umsatz, Gewinn, Bankbewegungen sowie Kontoständen und Kreditwürdigkeit.
- Buchführungsunterlagen, (unveröffentlichte) Jahresabschlüsse, Bilanzen, Geschäfts- und sonstige Finanzberichte.
- Kundenlisten und (End-)Kunden betreffende Informationen.
- Informationen und Listen zu Lieferanten, Dienstleistern oder anderen Geschäftspartnern sowie vertraulichen Geschäftsbeziehungen.
- Mitarbeiterlisten, Informationen zu Mitarbeitern, Personalplanung, Personalstrukturen und diesbezüglichen Prozessen.
- Business- und Geschäftsideen, Geschäftsstrategien, Kalkulationen, Marktdaten sowie Organisations- und Verfahrensstrukturen.
- KI-Modelle und/oder deren Feinabstimmung, wobei ein „KI-Modell“ die Software, Datenbank und den Algorithmus bezeichnet, d. h. das funktionale Fundament einer KI, das durch Training und/oder Programmierung erstellt wird und ihre Funktionalität sowie ihren Betrieb bestimmt, ebenso wie die Art und Weise, wie Eingaben verarbeitet und Ausgaben generiert werden. Es umfasst auch Maßnahmen zur Anpassung und Modifikation eines bestehenden KI-Modells für spezifische Zwecke.
- Besondere Markt- und Branchenkenntnisse, Marketingverfahren, Marketingideen sowie geplante Marketingmaßnahmen.
- Planungs-, Entwicklungs-, Produktions- und Produktbeobachtungsverfahren.
- Prompts und andere Anweisungen für Künstliche Intelligenz (KI), deren Erstellung einen erheblichen zeitlichen, finanziellen oder personellen Aufwand erfordert, gelten als Geschäftsgeheimnisse. Dazu zählen Prompts, die spezielles Wissen und Fachkenntnisse enthalten und nicht auf allgemein zugänglichen Vorlagen oder Anleitungen basieren.
- Prototypen, Muster, Formen, Rohdaten, Vorlagen, Entwürfe und Konzepte.
- Rezepte, Stoffzusammensetzungen, Materialbeschaffenheit und Beistoffe.
- Rechtsstreitigkeiten, Amts- und Gerichtsverfahren (z. B. mit Wettbewerbern, Behörden oder anderen Vertragsparteien).
- Maschinen-, Objekt- und Quellcode, Funktionen, Algorithmen, Lösungswege, Datenbanken, deren Struktur, Logik und Inhalte, strukturelle und grafische Gestaltung von Software und Softwareoberflächen, inklusive Konzeptions- und Entwurfsmaterial wie Ablaufplänen oder Struktogrammen.
- Technisches Know-how, nicht abgeschlossene Registrierungsverfahren für geistige und gewerbliche Schutzrechte (z. B. Urheber, Marken- und Patentrechte), nicht registrierte Patente und Erfindungen.
- Inhalte und Ausgestaltung von Schulungsunterlagen sowie Schulungsverfahren.
- Vorlagen, Vorschriften sowie Zeichnungen technischer Art.
- Verträge, Absprachen, Angebote, Konditionen, Vereinbarungen, Erklärungen, Verpflichtungen sowie deren Beteiligte und Inhalte, auch in der Anbahnungsphase und nach deren Beendigung.
- Inhalte von Ausschreibungen und Aufrufen zur Vorlage von Angeboten, insbesondere im Hinblick auf die erforderlichen Leistungen, Preise und andere Konditionen.
- Inhalte von Angeboten, Ausschreibungen und Pitches, insbesondere im Hinblick auf die angebotenen Leistungen, Preise und Konditionen sowie Verhandlungstaktiken.
- Zutritts-, Zugriffs- und Zugangsinformationen (z. B. Passwörter oder Zugangscodes).

Der Informationsempfänger wird darauf hingewiesen, dass die folgenden Ausnahmen und insbesondere die Erforderlichkeit der Offenlegung im konkreten Umfang, grundsätzlich von dem Informationsempfänger nachzuweisen sind.

- Die Information ist zum Zeitpunkt ihrer Offenlegung durch den Informationsempfänger allgemein bekannt oder öffentlich, d. h. jedermann zugänglich.
- Die Information wurde von dem Informationsempfänger eigenständig und unabhängig von den von dem Informationsinhaber erlangten Informationen entwickelt, bzw. geschaffen.
- Die Information wurde von dem Informationsempfänger ohne Verletzung gesetzlicher und vertraglicher Pflichten rechtmäßig erlangt.
- Der Informationsempfänger ist aufgrund einer Rechtsvorschrift oder behördlichen Anordnung zur Offenlegung der Information verpflichtet.

Anhang 2: Mindestanforderungen Technische und Organisatorische Maßnahmen (TOM) für Auftragnehmer

1. VERPFLICHTUNGEN UND RAHMENBEDINGUNGEN FÜR AUFTRAGNEHMER

Die Verpflichtung von Auftragnehmern auf die Vertraulichkeit und die Einhaltung von Mindestanforderungen im Bereich der Informationssicherheit und des Datenschutzes soll einen angemessenen Schutz der Informationswerte des Auftraggebers gewährleisten. Dabei wird ein Mindestniveau von Schutzmaßnahmen festgeschrieben, welches von jedem Auftragnehmer im Hinblick auf dessen IT-Systeme und Prozesse zu erfüllen ist.

Die vom Auftragnehmer umzusetzenden technischen und organisatorischen Maßnahmen ergeben sich aus:

- den für die konkrete Leistung jeweils relevanten Vertrag im Rahmen der Geschäftsbeziehung geschlossenen Vertrag (Hauptvertrag) einschließlich sämtlicher Anlagen (bspw. Leistungsbeschreibungen) und ergänzend
- den nachfolgend aufgeführten technischen und organisatorischen Maßnahmen.

Die folgenden Mindestanforderungen sind von allen Auftragnehmern einzuhalten, die Zugriff auf Informationen und personenbezogene Daten des Auftraggebers erhalten; weitergehende oder zusätzliche Maßnahmen, die im Hauptvertrag oder dessen Anlagen festgelegt sind, sind ebenfalls verbindlich umzusetzen. Diese Anforderungen bilden einen integralen Bestandteil des Vertragsverhältnisses. Bei Widersprüchen haben die Regelungen des Hauptvertrags einschließlich seiner Anlagen Vorrang vor den nachfolgend aufgeführten Maßnahmen.

Der Auftraggeber ist berechtigt, die Einhaltung der Maßnahmen zu überprüfen.

Zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber kann der Auftraggeber auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach ISO/IEC 27001) anfordern.

ÜBERSICHT UND ANWENDUNGSBEREICH DER ZUGRIFFS- UND VERARBEITUNGSTYPEN

Die hier beschriebenen technischen und organisatorischen Maßnahmen gelten als Mindest-Standard und dürfen nicht unterschritten werden. Sie gelten abhängig vom Zugriffs- oder Verarbeitungstyp (A–C):

Zugriffs- und Verarbeitungstyp	Beschreibung
A	Verarbeitung auf Systemen des Auftragnehmers (z. B. Cloud, Hosting, Outsourcing)
B	Zugriff des Auftragnehmers mit eigenen Endgeräten auf Systeme des Auftraggebers
C	Verwendung von Endgeräten und Systemen des Auftraggebers

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN: KATEGORIEN UND ANFORDERUNGEN

Kategorie	Beschreibung der Maßnahmen	gilt für
Organisation des Datenschutzes und der Informationssicherheit	Es bestehen klare Verantwortlichkeiten für Datenschutz und Informationssicherheit (ISB, DSB). Richtlinien und Prozesse sind dokumentiert, kommuniziert und werden regelmäßig überprüft.	A
	Sicherheitskonzepte und -maßnahmen sind implementiert und werden regelmäßig überprüft.	A, B
	Alle Mitarbeitenden und eingesetzte Unterauftragnehmer sind auf die Vertraulichkeit verpflichtet und werden regelmäßig geschult.	A - C
Physische Sicherheit und Zutrittsschutz	Es sind physische Sicherheitskontrollen für Büros, Räume und Einrichtungen konzipiert und umgesetzt. Sicherheitsmaßnahmen und Zutrittsrechte entsprechend den jeweiligen Sicherheitsanforderungen.	A - C
	Es existiert ein dokumentiertes Verfahren zur Vergabe, Änderung und zum Entzug von Zutrittsrechten einschließlich der Rückgabe von Zutrittsmitteln.	
	In Rechenzentren sind Schutzmaßnahmen gegen technische Beeinträchtigungen und Elementarschäden umgesetzt (u.a. USV, Klimaanlage, Schutz gegen Feuer und Wasser). Der Zutritt zu Rechenzentren ist auf den autorisierten Personenkreis beschränkt. Besucher werden begleitet und mit Datum und Uhrzeit Ihres Betretens und Verlassens erfasst. Es sind wirksame Zutrittsschutzmaßnahmen umgesetzt, einschließlich personengebundener, sicherer Zutrittsmittel, der Überwachung und Protokollierung von Zutritten sowie ein effektiver Einbruchschutz (EMA und VÜ).	A
Zugangs- und Zugriffssteuerung	Die Vergabe, Änderung und Genehmigung von Zugangs- und Zugriffsrechten unterliegen klar definierten Prozessen. Systemzugänge werden ausschließlich über personalisierte Konten bereitgestellt. Die Vergabe von Zugriffsrechten erfolgt nach dem „Need-to-Know“ und „least-privilege“ Prinzip. Accounts und Zugriffsrechte werden regelmäßig überprüft, inaktive Konten unverzüglich gesperrt, nicht erforderliche Zugriffe entzogen. Passwortvorgaben und Authentifizierungsverfahren entsprechen aktuellen Sicherheitsstandards. Privilegierte Konten (z.B. Systemadministratoren) werden durch starke Authentifizierung (z.B. MFA) geschützt, sind auf ein Minimum zu beschränken und werden streng überwacht. Administrator-Accounts dürfen nicht für normale Bürotätigkeiten verwendet werden.	A

	Arbeitsplätze sind durch automatische Bildschirmsperren zu schützen. Systemzugänge werden entweder gesichert oder gesperrt.	A, B
Verschlüsselung	Mobile Endgeräte werden entsprechend dem Stand der Technik verschlüsselt.	A, B
	Eine Datenübertragung über öffentliche Netze oder anderweitig nicht vertrauenswürdige Netze erfolgt ausschließlich über verschlüsselte Verbindungen (TLS, VPN).	A, B
Transport und Entsorgung von Datenträgern	Externe elektronische Medien (bspw. tragbare Festplatten, Band, USB-Sticks) werden bei Transporten außerhalb des Bereiches des Auftragnehmers in gesicherten, verschlossenen Transportbehältnissen durch spezielle Kurierdienste transportiert oder durch Verfahren wie Verschlüsselung gesichert. Bei der Datenlöschung und Vernichtung von Datenträgern sind die Vorgaben der ISO 21964 einzuhalten.	A
System- und Betriebssicherheit	Informationen über technische Schwachstellen zu den genutzten IT-Systemen werden gesammelt (z. B. Information vom Hersteller, System-Audits, CVS-Datenbank) und bewertet (z. B. Common Vulnerability Scoring System CVSS). Potenziell betroffene IT-Systeme und Software werden identifiziert, beurteilt und Schwachstellen behandelt. Systeme (Betriebssysteme, Anwendungen, Netzkomponenten) werden regelmäßig auf bekannte Schwachstellen hin analysiert. Aufgedeckte Schwachstellen und Ergebnisse werden in geeigneter Weise analysiert, klassifiziert und behoben. Abhilfemaßnahmen werden entsprechend ihrer Kritikalität zeitnah umgesetzt. Es existiert ein definierter Patch-Management-Prozess, der sicherstellt, dass auf der vom Auftragnehmer eingesetzten Hardware ausschließlich korrekt lizenzierte Software verwendet wird und alle Systeme regelmäßig mit aktuellen Sicherheits-Patches versorgt werden. Hardware (z. B. Clients, Server, Gateways), die zur Leistungserbringung eingesetzt wird, wird durch angemessene, aktuelle Anti-Malware-Software geschützt. Die Software erkennt, wenn der Schutz deaktiviert ist oder nicht regelmäßig aktualisiert wird. Bei Erkennung einer Bedrohung erfolgt eine automatisierte Alarmierung und eine angemessene, nachvollziehbare Bearbeitung. IT-Ressourcen (z. B. Datenbanken, Anwendungen, Betriebssysteme, Netzwerkgeräte) werden auf Basis sicherer Grundlagen (Härtung) konfiguriert und betrieben. Die Sicherheitsstandards orientieren sich an Best Practices, wie den CIS-Standards oder gleichwertigen Verfahren. Konfigurationen der IT-Anlagen werden regelmäßig überprüft und aktualisiert. Es werden risikobasierte Protokollierungs- und Überwachungsmaßnahmen etabliert, die relevante System-, Netzwerk- und Benutzeraktivitäten erfassen. Der Detailgrad richtet sich nach der Sensibilität der Information und der Systemkritikalität	A, B

	und ermöglicht die Nachvollziehbarkeit von Änderungen, auch an personenbezogenen Daten. Ereignisdaten aus Endgeräten und Netzwerkzonen werden zentral zusammengeführt und kontinuierlich auf Sicherheitsereignisse ausgewertet.	
	Es existieren formale Richtlinien für das Change-Management und den Lebenszyklus der sicheren Softwareentwicklung, die sicherheitsrelevante Kontrollen festlegen. Sicherheitsüberprüfungen bei neuen Systemdesigns oder Änderungen sowie Sicherheitstests vor der Bereitstellung sind fester Bestandteil der Prozesse. Änderungen werden erst nach angemessener Anforderung, Autorisierung, Testung und Genehmigung für die Produktion freigegeben.	A
	Trennungskontrolle Umgebungen sind physisch oder logisch getrennt. Insbesondere bei gemeinsam mit anderen Auftraggebern genutzten Umgebungen sowie beim Betrieb von Test-, Qualitäts- und Produktionsumgebungen.	A

Netzwerksicherheit	Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen sind voneinander zu trennen (z. B. durch Firewalls). Netzwerkperimeter müssen durch Firewalls geschützt sein, und Firewall Regeln einen dokumentierten Freigabeprozess durchlaufen. Authentisierungsmerkmale (z. B. Passwörter, PINs) werden ausschließlich verschlüsselt übertragen. Aus dem Internet erreichbare administrative Zugänge oder technische Netzwerk Ports sind abzuschalten oder angemessen abzusichern (z. B. mittels Zwei-Faktor-Authentisierung).	A
Backup und Wiederherstellung	Sicherungs- und Datenhaltungskonzepte für alle relevanten Plattformen und Komponenten im Verantwortungsbereich des Auftragnehmers sind implementiert und umgesetzt. Aufbewahrungsfristen sind definiert, Backups sowie Wiederherstellungstests werden nachweisbar durchgeführt. Die Sicherungskonzepte und Wiederherstellungsverfahren sind so ausgelegt, dass die vereinbarten Verfügbarkeitsstufen gewährleistet werden.	A
IT-Notfallmanagement	Notfallkonzepte und Wiederanlaufpläne sind dokumentiert, getestet und enthalten klare Rollen und Kommunikationswege.	A
Vorfallmanagement	Es existieren dokumentierte Verfahren für Informationssicherheits- und Datenschutzvorfälle, die eine wirksame und ordnungsgemäße Behandlung sicherstellen. Die Verfahren umfassen Meldung, Analyse, Überwachung, Lösung und Dokumentation von Vorfällen sowie Reaktions- und Wiederherstellungsprozesse. Datenschutzvorfälle und Vorfälle mit Auswirkungen auf die Leistungserbringung werden dem Auftraggeber unverzüglich gemeldet.	A, B
Lieferantenmanagement	Mit allen Unterauftragnehmern bestehen verbindliche Vereinbarungen, die ihre Verantwortung für die Sicherheit, der im Auftrag des Auftraggebers verarbeiteten, gespeicherten oder übermittelten Daten festlegen. Ihre Sicherheitsmaßnahmen müssen mindestens dem in diesem Dokument und im Hauptvertrag definierten Schutzniveau entsprechen. Einhaltung und Wirksamkeit werden im Rahmen des Lieferantenmanagements durch den Auftragnehmer regelmäßig überprüft.	A - C