Unternehmensrichtlinie Datenschutz
enna systems GmbH

Dokumenteninformationen

Klassifikation:	Intern		
Versionsnummer:	1.0		
Dokumententitel:	Unternehmensrichtlinie Datenschutz		
Dokumentenverantwortlicher:			
Erstellt am:	10.04.2024	**Erstellt von:**	Tobias Bily
		Funktion des Erstellers:	Datenschutzkoordinator
Letzte Überarbeitung:	10.04.2024	**Nächste Überarbeitung:**	10.04.2025
Freigabe am:	11.04.2024	**Freigabe von:**	Tim Haug

Dokumentenverteiler

Berechtigte Rollen (Verteilerkreis)
Geschäftsleitung
Mitarbeiter

Versionsverlauf

Datum	**Version**	**Beschreibung**	**Verändert durch**
	1.0	Erstellung	Tobias Bily

Inhaltsverzeichnis

§ 1 Bedeutung, Ziel, Zugänglichkeit 1

§ 2 Geltungsbereich 1

§ 3 Begriffsbestimmungen 1

§ 4 Rollen und Verantwortlichkeiten 3

§ 5 Datenschutzbeauftragter 3

§ 6 Umgang mit personenbezogenen Daten 3

§ 7 Besondere Kategorien personenbezogener Daten 4

§ 8 Datenübermittlung 5

§ 9 Externe Dienstleister/Kooperationen 5

§ 10 Datenminimierung, Privacy by Design/Privacy by Default 5

§ 11 Rechte von Betroffenen 6

§ 12 Auskunftsersuchen Dritter über Betroffene 7

§ 13 Verfahrenseinführungen und -prüfungen 7

§ 14 Verzeichnis von Verarbeitungstätigkeiten 7

§ 15 Werbung 7

§ 16 Schulung 8

§ 17 Datengeheimnis 8

§ 18 Beschwerden 8

§ 19 Audits 8

§ 20 Interne Ermittlungen 8

§ 21 Verfügbarkeit, Vertraulichkeit und Integrität von Daten 9

§ 22 Datenschutz-Folgenabschätzung 9

§ 23 Verletzungen des Schutzes von Daten („Datenpanne“) 10

§ 24 Folgen von Verstößen 10

§ 25 Rechenschaftspflicht 10

§ 26 Aktualisierung der Richtlinie; Nachweisbarkeit 10

§ 1 Bedeutung, Ziel, Zugänglichkeit

1.1. Die im Unternehmen vorhandenen Daten sind für das Unternehmen und die reibungslosen Abläufe im Unternehmen von großem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen.

1.2. Gleichzeitig erwarten die Kunden, Partner und Mitarbeiter des Unternehmens, dass die dem Unternehmen anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt.

1.3. Das Unternehmen bekennt sich auch im Rahmen seines gesellschaftlichen Engagements zu seiner Verantwortung für den sorgsamen Umgang mit personenbezogenen Daten.

1.4. Mit dieser Unternehmensrichtlinie sollen einheitliche Standards für den Datenschutz im Unternehmen geschaffen werden.

1.5. Durch die Einhaltung der in dieser Richtlinie definierten Standards kommt das Unternehmen seinen datenschutzrechtlichen Verpflichtungen nach und sorgt für eine ausreichende Berücksichtigung der Interessen sowie Rechte der betroffenen Personen.

1.6. Die Beachtung dieser Richtlinie ist Voraussetzung für den sicheren Austausch von personenbezogenen Daten innerhalb des Unternehmens.

1.7. Die Richtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

§ 2 Geltungsbereich

2.1. Diese Richtlinie findet Geltung für das Unternehmen enna systems GbH, Sandstraße 35, 80335 München.

2.2. Sie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten des Unternehmens.

2.3. Die Gebote und Verbote dieser Unternehmensrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig davon, ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von Betroffenen (Kunden, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein. Details zum Umgang mit personenbezogenen Daten werden in Verfahrensanweisungen und Prozessbeschreibungen festgelegt, welche die jeweiligen Pflichten genau definieren.

§ 3 Begriffsbestimmungen

3.1. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z.B. beim Autokennzeichen. Das Zustandekommen und die Art bzw. Verkörperung der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

3.2. Besondere Kategorien personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person. Auch personenbezogene Daten zu strafrechtlichen Verurteilungen und Straftaten oder damit zusammenhängenden Sicherungsmaßregeln stehen unter einem besonderen gesetzlichen Schutz.

3.3. Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

3.4. Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Personenbezogene Daten können beispielsweise auch in ihrer Verarbeitung eingeschränkt werden, wenn sie in ein Archivsystem überführt werden.

3.5. Ein Verfahren stellt einen Ablauf von Verarbeitungsschritten dar, mit denen eine oder mehrere (vom Standpunkt des Verantwortlichen und des Betroffenen aus betrachtet) miteinander verbundene Zweckbestimmungen realisiert werden sollen. So sind beispielsweise die Personalverwaltung oder die Videoüberwachung erfasst. Aber selbst eine einzelne Applikation kann ein Verfahren darstellen, wenn hierdurch ein eigenständiger Zweck verfolgt werden soll.

3.6. Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Die Analyse des Surfverhaltens von Kunden auf der Webseite des Unternehmens kann beispielsweise ein Profiling darstellen.

3.7. Als automatisierte Einzelentscheidung werden Entscheidungen über einen Menschen bezeichnet, die ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhen und diese Entscheidung gegenüber dem Betroffenen eine rechtliche Wirkung entfaltet oder diesen in ähnlicher Weise beeinträchtigt. Beispielsweise liegt eine automatisierte Einzelfallentscheidung vor, wenn durch das Unternehmen Bewerberfragebögen automatisiert ausgewertet und nur diejenigen Bewerber, die eine bestimmte Punktzahl erreicht haben, zum Bewerbungsgespräch eingeladen werden.

3.8. Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Eine einfache Form der Pseudonymisierung ist das Ersetzen von Identifikationsmerkmalen (z.B. Name und Anschrift) mit einer individuellen Kennnummer.

3.9. Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In der Regel ist das Unternehmen ein Verantwortlicher für eine Verarbeitung.

3.10. Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Dem Auftragsverarbeiter steht keine Befugnis zu, selbst über die Zwecke der Verarbeitung personenbezogener Daten des Verantwortlichen zu entscheiden.

3.11. Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten (s. den nachfolgenden Absatz) handelt oder nicht.

3.12. Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

3.13. Eine Einwilligung des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

Hinsichtlich der Ausgestaltung und Form der Einwilligung ist der Datenschutzbeauftragte beizuziehen. Einwilligungen sind aufgrund bestehender Rechenschaftspflichten des Unternehmens stets zu dokumentieren.

3.14. Das Verzeichnis von Verarbeitungstätigkeiten ist eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen, einen Nachweis hinsichtlich der Erfüllung der gesetzlichen Vorgaben zum Datenschutz zu erbringen.

§ 4 Rollen und Verantwortlichkeiten

4.1. Die Geschäftsführung des Unternehmens hat dafür Sorge zu tragen, dass im Unternehmen ein Datenschutzmanagement und IT-Sicherheitsmanagement etabliert ist. Sie ist insgesamt für die Einhaltung des Datenschutzes verantwortlich.

Die Umsetzung des Datenschutzes wird durch den Aufbau einer entsprechenden Struktur sichergestellt:

4.2. Für jede Verarbeitung personenbezogener Daten ist ein Verfahrensverantwortlicher zu bestimmen. Der Verfahrensverantwortliche führt die Anweisungen der Geschäftsführung zur Umsetzung der gesetzlichen Vorgaben zum Datenschutz aus. Er trägt die Verantwortung für das jeweilige Verfahren und hat dafür zu Sorge zu tragen, dass die gesetzlichen Anforderungen zum Datenschutz sowie Anforderungen aus dieser Richtlinie im jeweiligen Verfahren eingehalten werden (insbesondere Privacy by Design/by Default, Löschkonzepte, Erfüllung gesetzlicher Transparenzpflichten, arbeitsplatzbezogene Instruktion des einzelnen Mitarbeiters oder die frühzeitige Einbindung des Datenschutzbeauftragten etc.).

4.3. Jeder Mitarbeiter hat im Rahmen der Verarbeitung personenbezogener Daten folgende Pflichten:

- das Vertrautmachen mit internen Regelungen und gesetzlichen Vorschriften zum Datenschutz und die Einhaltung dieser Vorgaben
- das Zuratеziehen des Datenschutzbeauftragten in datenschutzrechtlichen Zweifelsfällen
- die Meldung von Datenpannen (vgl. § 23)

§ 5 Datenschutzbeauftragter

5.1. Der Datenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz, einschließlich der Anforderungen dieser und anderer Richtlinien des Unternehmens zum Datenschutz. Er berät und unterrichtet die Unternehmensleitung hinsichtlich bestehender Datenschutzpflichten und ist für die Kommunikation mit Aufsichtsbehörden zuständig. Ausgewählte Prozesse werden durch ihn stichprobenartig, risikoorientiert und in angemessenen Zeitabständen auf ihre Datenschutzkonformität hin kontrolliert.

5.2. Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet unmittelbar der Geschäftsführung.

5.3. Das Unternehmen bzw. seine Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

5.4. Das Unternehmen hat einen Datenschutzbeauftragten bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten:

Dr. Adina Weiss

Business Campus
Parkring 49
85748 Garching b. München
Tel.: +49 89 61421070
E-Mail: dsb-enna@weiss-datenschutzrecht.de

§ 6 Umgang mit personenbezogenen Daten

6.1. Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der DSGVO grundsätzlich verarbeitet werden:

- Bei einem bestehendes Vertragsverhältnis mit dem Betroffenen.

  Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Darlehensvertrages.

- Im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen.

  Beispiel: Kunde K fordert Informationen zu Produkt X an und erwirbt dieses. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung des Geschäfts (Lieferung der Ware sowie Zahlung des Kaufpreises) dürfen verarbeitet werden.

- Wenn und soweit der Betroffene eingewilligt hat.

  Beispiel: Der Betroffene meldet sich zum Erhalt eines Newsletters an.

- Wenn eine rechtliche Verpflichtung besteht, der das Unternehmen unterliegt.

  Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).

- Wenn berechtigte Interessen des Unternehmens bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch den Datenschutzbeauftragten vorgenommen werden.

  Beispiel: Die Nutzung der postalischen Anschrift zur Aussendung von Werbeschreiben.

6.2. Betroffene dürfen nicht einer ausschließlich auf einer automatisierten Verarbeitung – so auch dem Profiling – beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Der Verfahrensverantwortliche stimmt solche Verarbeitungen vorab mit dem Datenschutzbeauftragten ab.

6.3. Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

6.4. Falls möglich, sollte auf einen Umgang mit personenbezogenen Daten verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

6.5. Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch den Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die

Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

6.6. Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger seiner personenbezogenen Daten sowie alle sonstigen Informationen i.S.d. Art. 13 DSGVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen. Falls notwendig, kann die Information in abgestufter Form bereitgestellt werden, so z.B. über Verlinkung auf eine ausführliche Datenschutzerklärung für die Verarbeitung.

6.7. Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern werden beispielsweise bei einem anderen Unternehmen beschafft, ist der Betroffene nachträglich (spätestens nach einem Monat) und umfassend gem. Art. 14 DSGVO über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung (Art. 13 Abs. 3 DSGVO).

6.8. Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

§ 7 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten dürfen grundsätzlich nur mit ausdrücklicher Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z.B. Verschlüsselung beim Transport, eingeschränkte Zugriffsrechte) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 8 Datenübermittlung

8.1. Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

8.2. Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder nicht hergestellt werden kann (beispielsweise über besondere Vertragsklauseln).

8.3. Übermittlungen personenbezogener Daten in ein Drittland sind vorab mit dem Datenschutzbeauftragten abzustimmen.

§ 9 Externe Dienstleister/Kooperationen

9.1. Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

9.2. Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Anbieters im Markt
- sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc..).

9.3. Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

9.4. Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

9.5. Für den Fall, dass mit einem oder mehreren Verantwortlichen gemeinsam über die Zwecke und Mittel einer Verarbeitung personenbezogener Daten entschieden werden soll (z.B. im Rahmen einer Kooperation), muss zwischen den gemeinsam für die Verarbeitung Verantwortlichen ein Vertrag geschlossen werden, der die Rollen und Aufgaben zur Einhaltung der gesetzlichen Vorgaben zum Datenschutz innerhalb des gemeinsamen Unterfangens transparent wiedergibt.

§ 10 Datenminimierung, Privacy by Design/Privacy by Default

10.1. Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung“). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

10.2. Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

§ 11 Rechte von Betroffenen

11.1. Betroffene haben das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten.

11.2. Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

11.3. Die Auskunftserteilung erfolgt schriftlich, es sei denn, der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DSGVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest („Recht auf Datenübertragbarkeit“). Der Umfang der Datenkopie sowie die Frage, ob im Einzelfall ein Recht auf Datenübertragbarkeit besteht, sind mit dem Datenschutzbeauftragten abzustimmen.

11.4. Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

11.5. Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich (z.B. ein Bewerber wird abgelehnt)
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung

- ihre Verarbeitung ist unzulässig (z.B. besteht keine Rechtsgrundlage für die Verarbeitung)
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein (z.B. ein Newsletter wird abbestellt) oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht oder an Dritte übertragen, sind die Empfänger über das Löschbegehren des Betroffenen hinsichtlich seiner Daten, sowie im Falle einer erfolgten Veröffentlichung, auch hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

11.6. Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder
- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

11.7. Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

11.8. Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

§ 12 Auskunftsersuchen Dritter über Betroffene

12.1. Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise über Kunden oder Beschäftigte dieses Unternehmens, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft suchende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- eine gesetzliche Norm zur Auskunft verpflichtet, sowie
- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

12.2. Auskunftsersuchen von Dritten und deren Beantwortung sind zu dokumentieren.

§ 13 Verfahrenseinführungen und -prüfungen

13.1. Mit Erreichen eines konkreten Planungsstadiums einer beabsichtigten Verarbeitungstätigkeit (Verfahrens) meldet der Verfahrensverantwortliche die Verarbeitung an den Datenschutzkoordinator. Mithilfe des Formulars wird die Einhaltung der gesetzlichen Anforderungen, einschließlich einer Risikoklassifizierung sichergestellt.

13.2. Der Verfahrensverantwortliche wählt, ggf. unter Zurateziehung der IT-Abteilung, geeignete technische und organisatorische Maßnahmen aus, um sicherzustellen, dass die Anforderungen an Privacy by Design/Privacy by Default eingehalten werden (vgl. § 10).

13.3. Die Verarbeitungstätigkeit wird durch den Verfahrensverantwortlichen im Verzeichnis der Verarbeitungstätigkeiten (vgl. § 14) dokumentiert. Der Verfahrensverantwortliche sorgt ggf. für weitere Dokumentationen, um die Einhaltung des Verfahrens mit den gesetzlichen Bestimmungen sowie den Bestimmungen dieser Richtlinie nachweisen zu können.

13.4. Der Verfahrensverantwortliche nimmt in regelmäßigen Abständen sowie anlassbezogen (z.B. bei einer Datenpanne, einer Beschwerde eines Betroffenen oder beim Erkennen falscher bzw. unvollständiger Angaben in den Verfahrensdokumentationen) eine Überprüfung bestehender Verfahren vor:

- Verfahren mit einer Risikoklassifizierung „gering“ alle drei Jahre
- Verfahren mit einer Risikoklassifizierung „mittel“ alle zwei Jahre
- Verfahren mit einer Risikoklassifizierung „hoch“ jährlich

Die Prüfung beinhaltet die Wirksamkeit der getroffenen technisch-organisatorischen Maßnahmen sowie die Aktualität der Angaben für das Verzeichnis von Verarbeitungstätigkeiten.

§ 14 Verzeichnis von Verarbeitungstätigkeiten

14.1. Das Unternehmen hat ein Verzeichnis über alle Datenverarbeitungen zu führen. Jede Fachabteilung hat einen Verfahrensverantwortlichen zu benennen, der alle notwendigen Informationen zu den Verfahren der jeweiligen Abteilung nach den gesetzlichen Anforderungen des Art. 30 DSGVO dokumentiert. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

14.2. Das Unternehmen stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit der Geschäftsführung.

§ 15 Werbung

15.1. Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

15.2. Ausnahmen sind nur bei Vorliegen einer Erlaubnisnorm zulässig. Diesbezüglich ist der Datenschutzbeauftragte zu konsultieren.

15.3. Ist eine Verarbeitung personenbezogener Daten zu Werbezwecken beabsichtigt, ist der Betroffene, neben den notwendigen Angaben nach Art. 13 DSGVO, spätestens bei der ersten Kommunikation auf sein Widerspruchsrecht in hervorgehobener Form (z.B. Fettdruck) hinzuweisen. Eingelegte Widersprüche hinsichtlich der werblichen Ansprache sind verpflichtend und ohne weitere Prüfung umzusetzen. Eine Sperrliste ist zur Identifikation eingelegter Widersprüche vom jeweiligen Verfahrensverantwortlichen anzulegen.

§ 16 Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die Geschäftsführung entscheidet über Form und Turnus der entsprechenden Schulungen in Absprache mit dem Datenschutzbeauftragten.

§ 17 Datengeheimnis

17.1. Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Es ist nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der übertragenen Aufgaben erforderlich ist. Beschäftigte sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch die Geschäftsleitung unter Verwendung des hierzu vorgesehenen Formulars.

17.2. Mitarbeiter mit besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis) werden von der Unternehmensleitung ergänzend schriftlich darauf verpflichtet.

§ 18 Beschwerden

18.1. Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.

18.2. Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzbeauftragte als unabhängige und weisungsfreie interne Instanz.

§ 19 Audits

19.1. Um ein hohes Datenschutzniveau zu gewährleisten, werden relevante Prozesse durch regelmäßige Audits interner Stellen oder durch externe Auditoren überprüft. Im Falle der Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemaßnahmen zu treffen.

19.2. Die beim Audit gewonnenen Erkenntnisse sind zu dokumentieren. Die Dokumentation ist dem Datenschutzbeauftragten, der Unternehmensleitung sowie den Fachverantwortlichen für den jeweiligen Prozess zu übergeben.

19.3. Ein Audit ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Maßnahmen umgesetzt sind. Bei Bedarf werden Follow-up-Audits durchgeführt, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

§ 20 Interne Ermittlungen

20.1. Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismäßig sein.

20.2. Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

20.3. Bei allen Formen der internen Ermittlungen ist der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen.

§ 21 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

21.1. In Abhängigkeit von der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

21.2. Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

21.3. Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

21.4. Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von zehn Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht

zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Unternehmen oder dem jeweiligen Nutzer stehen.

21.5. Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein. Jede Zugriffsberechtigung ist durch einen Verfahrensverantwortlichen zu genehmigen.

21.6. Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls es der Schutzbedarf der personenbezogenen Daten erfordert.

21.7. Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Eine Trennung kann auf logischer Ebene (z.B. innerhalb einer Datenbank) oder auf physikalischer Ebene (z.B. durch Verarbeitung in unterschiedlichen Systemen) vorgenommen werden.

21.8. Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

21.9. Das Unternehmen hat einen Informationssicherheitsbeauftragten benannt. Diesen erreichen Sie unter folgenden Kontaktdaten:

Timo Köhler
t.koehler@enna.care
Tel.: +49 160 947 113 83

§ 22 Datenschutz-Folgenabschätzung

22.1. Jede Fachabteilung ist zur Durchführung von Datenschutz-Folgenabschätzungen für Verfahren, die unter ihrer Verantwortung erfolgen, vor der Verarbeitung personenbezogener Daten verpflichtet, wenn ein hohes Risiko für Rechte und Freiheiten von Betroffen aufgrund der Datenverarbeitung zu erwarten ist. Bei der Datenschutz-Folgenabschätzung werden Risiken für Betroffene und deren Eintrittswahrscheinlichkeit ermittelt, bewertet und dokumentiert. Die Datenschutz-Folgenabschätzung hat alle gesetzlich geforderten Beschreibungen des Art. 35 Abs. 7 DSGVO zu enthalten.

22.2. Der Datenschutzbeauftragte berät die Fachabteilungen bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für Betroffene beinhalten können.

§ 23 Verletzungen des Schutzes von Daten („Datenpanne“)

23.1. Sollten personenbezogene Daten unrechtmäßig Dritten offenbart worden sein (z.B. wurden Daten an einen falschen Empfänger übermittelt oder ein IT-System bzw. eine Applikation wurden kompromittiert), sollten personenbezogene Daten versehentlich geändert oder nicht mehr verfügbar sein, ist darüber unverzüglich das unternehmensinterne Incident Response Team zu informieren. Das Incident Response Team bezieht unverzüglich den Datenschutzbeauftragten im Rahmen der Sachverhaltsaufklärung ein. Die Kontaktdaten des Incident Response Teams lauten wie folgt: Tim Haug, t.haug@enna.care, +49 177 4200787

23.2. Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

23.3. Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch den Datenschutzbeauftragten. Betroffene werden durch die Geschäftsleitung informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 24 Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 25 Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

§ 26 Aktualisierung der Richtlinie; Nachweisbarkeit

26.1. Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

26.2. Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.