Datenschutz-Anlage GBS Cloud-Dienste (“DSA”)

1 Präambel

Die Parteien vereinbaren, dass diese Anlage zum Datenschutz ("DSA") ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von Kundendaten und personenbezogenen Daten im Zusammenhang mit den vom Anbieter angebotenen Dienstleistungen festlegt. Die DSA wird durch Verweis in die AGB GBS und die AGB GBS Cloud-Dienste aufgenommen.

Im Falle eines Widerspruchs oder einer Widersprüchlichkeit zwischen diesen DSA-Bedingungen und anderen Bestimmungen in den Allgemeinen Geschäftsbedingungen haben diese DSA-Bedingungen Vorrang.

Der Anbieter wird alle Gesetze und Vorschriften einhalten, die für die Erbringung seiner Dienstleistungen gelten, einschließlich der Datenschutzanforderungen. Zur Klarstellung: Der Anbieter ist nicht verantwortlich für die Einhaltung von Gesetzen oder Vorschriften, die auf den Kunden oder die Branche des Kunden anwendbar sind und die nicht allgemein auf die Dienstleistungen anwendbar sind, die der Anbieter dem Kunden zur Verfügung stellt. Der Anbieter bestimmt nicht, ob Kundendaten Informationen enthalten, die bestimmten Gesetzen oder Vorschriften unterliegen.

Der Kunde wird alle Gesetze und Vorschriften einhalten, die auf seine Nutzung der Dienstleistung anwendbar sind, einschließlich, aber nicht beschränkt auf Gesetze in Bezug auf Vertraulichkeit und Datenschutz.

2 Definitionen

Begriffe, die in dieser DSA verwendet, aber nicht definiert werden, haben die in den Allgemeinen Geschäftsbedingungen angegebenen Bedeutungen. Die nachstehenden Definitionen haben folgende Bedeutung:

"**Datenschutzanforderungen**" bedeutet die DSGVO, die lokalen Datenschutzgesetze und alle anwendbaren Gesetze, Vorschriften und andere gesetzliche Anforderungen in Bezug auf Datenschutz und Datensicherheit sowie die Verwendung, Sammlung, Aufbewahrung, Speicherung, Sicherung, Offenlegung, Übertragung, Entsorgung und andere Arten von Verarbeitung personenbezogener Daten.

"**Diagnostische Daten**" bedeutet eine bestimmte Art von Daten, die bei der Untersuchung und Diagnose von IT-Systemproblemen verwendet werden, Transaktionsleistung, Fehler oder fehlerhafte Ausgabe.

DSGVO bedeutet Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Allgemeine Datenschutzverordnung).

"**Kundendaten**" bezeichnet alle Daten, einschließlich, aber nicht beschränkt auf alle Text-, Ton-, Video- oder Bilddateien und Software, die dem Anbieter vom oder im Namen des Kunden durch die Nutzung der Dienstleistung zur Verfügung gestellt werden.

"**Lokale Datenschutzgesetze**" sind alle untergeordneten Gesetze und Vorschriften zur Umsetzung der DSGVO.

"**Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Eine **identifizierbare natürliche Person** ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf eine Kennung wie einen Namen, eine Kennnummer, Standortdaten, eine Online-Kennung oder auf einen oder mehrere spezifische Faktoren, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

"**Service-generierte Daten**" sind Daten, die vom Anbieter durch den Betrieb eines Online-Dienstes generiert oder abgeleitet werden. Service-generierte Daten umfassen keine Kundendaten, Diagnosedaten oder Daten zu professionellen Dienstleistungen.

"**Standardvertragsklauseln**" sind die Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer, die kein angemessenes Datenschutzniveau gewährleisten, wie in Artikel 46 der DSGVO beschrieben.

"**Supportdaten**" sind alle Daten, einschließlich aller Text-, Ton-, Video-, Bilddateien oder Software, die dem Anbieter vom oder im Namen des Kunden zur Verfügung gestellt werden (oder die der Kunde dem Anbieter autorisiert, von einem Online-Service zu beziehen), und zwar durch eine Vereinbarung mit dem Anbieter, um technischen Support für Online-Services zu erhalten, der unter die Allgemeinen Geschäftsbedingungen fällt.

"**Unterauftragsverarbeiter**" bezeichnet andere Verarbeiter, die vom Anbieter zur Verarbeitung von Kundendaten und personenbezogenen Daten gemäß Artikel 28 der DSGVO einbezogen werden.

Alle spezifischen Datenschutzbestimmungen, die sich auf den Schutz personenbezogener Daten beziehen und in diesem Abkommen verwendet werden, haben die Bedeutung, die sie in der DSGVO und anderen anwendbaren Datenschutzgesetzen haben.

Zur Klarstellung und wie oben ausgeführt, können Daten, die als Kundendaten, Diagnosedaten und dienstleistungsgenerierte Daten definiert sind, personenbezogene Daten enthalten.

3 Umfang der DSA

Die in dieser DSA genannten Bedingungen gelten für alle Dienstleistungen, die der Anbieter für den Kunden erbringt, soweit Kunden- oder Personendaten betroffen sind.

Previews decken möglicherweise nicht die Datenschutz- und Sicherheitsmaßnahmen ab, die für die Dienstleistung angegeben sind. Der Kunde darf Previews nicht zur Verarbeitung persönlicher Daten oder anderer Daten verwenden, die gesetzlichen oder behördlichen Vorschriften unterliegen.

4 Datenschutzvorschriften

4.1 Verwendung der Daten und Datenverarbeitung

Der Anbieter verwendet und verarbeitet Kundendaten und personenbezogene Daten nur im Namen und auf Weisung des Kunden, um Dienstleistungen zu erbringen, und für den legitimen Geschäftsbetrieb des Anbieters im Zusammenhang mit der Lieferung der Dienstleistungen an den Kunden in dem im Folgenden beschriebenen Umfang. Der Kunde behält sich alle Rechte, Titel und

Interessen an den Kundendaten vor. Der Anbieter erwirbt keine Rechte an Kundendaten, mit Ausnahme der Rechte, die der Kunde dem Anbieter im Rahmen dieser DSA einräumt. Alle Weisungen sind vom Anbieter zu dokumentieren und dem Kunden auf Verlangen vorzulegen. Dieser Absatz hat keinen Einfluss auf die Rechte des Anbieters an Software oder Dienstleistungen, die der Anbieter dem Kunden lizenziert.

4.2 **Verarbeitung für die Bereitstellung von Dienstleistungen**

Für die Zwecke dieser DSA besteht die Bereitstellung der Dienstleistung aus:

- Sichere Kundenkommunikation;
- Suche nach schädlichem Inhalt; und
- Verbesserung der Produktivität.

Bei der Bereitstellung der Dienstleistungen wird der Anbieter Kundendaten oder persönliche Daten nicht für Benutzerprofile, Werbung oder ähnliche kommerzielle Zwecke oder Marktforschung verwenden oder anderweitig verarbeiten, es sei denn, eine solche Verwendung oder Verarbeitung erfolgt in Übereinstimmung mit den Weisungen des Kunden.

4.3 **Offenlegung von verarbeiteten Daten**

Der Anbieter wird keine verarbeiteten Daten offenlegen oder Zugang zu ihnen gewähren, außer auf Weisung des Kunden, wie in dieser DSA beschrieben oder wie gesetzlich vorgeschrieben. Für die Zwecke dieses Abschnitts bedeutet "verarbeitete Daten" Kundendaten, persönliche Daten und alle anderen Daten, die vom Anbieter im Zusammenhang mit der Dienstleistung verarbeitet werden und vertrauliche Informationen des Kunden darstellen. Die Verarbeitung der verarbeiteten Daten unterliegt der Vertraulichkeit gemäß den Allgemeinen Geschäftsbedingungen der Dienstleistung.

Der Anbieter gibt verarbeitete Daten nur dann an juristische Personen weiter oder gewährt ihnen Zugang zu diesen Daten, wenn dies gesetzlich vorgeschrieben ist. Sofern gesetzlich zulässig, wird der Anbieter den Kunden über die jeweilige Anfrage informieren.

Für den Fall, dass der Anbieter eine Anfrage eines Dritten nach verarbeiteten Daten erhält, wird der Anbieter, sofern gesetzlich zulässig, den Kunden über die entsprechende Anfrage informieren.

In beiden Fällen und im gesetzlich zulässigen Umfang wird der Anbieter versuchen, die Anfragen an den Kunden zu richten. Dem Anbieter ist es daher gestattet, die Kontaktinformationen des Kunden anzugeben.

4.4 **Rollen und Pflichten der Parteien**

Die Parteien stimmen überein, dass der Kunde, der für die personenbezogenen Daten Verantwortliche und der Anbieter der Verarbeiter der personenbezogenen Daten ist. Der Anbieter kann Unterauftragsverarbeiter in dem Umfang einsetzen, wie unter Art. 8 dieser DSA beschrieben. Der Anbieter wird personenbezogene Daten nur in dem Umfang verarbeiten, in dem er vom Kunden dokumentierte Weisungen erhalten hat.

Der Kunde erklärt sich damit einverstanden, dass die Allgemeinen Geschäftsbedingungen des Anbieters (einschließlich der zu diesem Zeitpunkt aktuellen DSA-Bedingungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Nutzung und Konfiguration von Funktionen in der Dienstleistung durch den Kunden die vollständigen dokumentierten Weisungen des Kunden an den Anbieter für die Verarbeitung personenbezogener Daten darstellen.

4.5 **Pflichten des Anbieters**

Der Anbieter ist verpflichtet, eine interne Organisation für den Schutz personenbezogener Daten einzurichten, die den Anforderungen der geltenden Gesetzgebung entspricht.

Der Anbieter ist verpflichtet, die technischen und organisatorischen Maßnahmen zu ergreifen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste gewährleisten.

Der Anbieter ist verpflichtet, ein Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.

Der Anbieter stellt sicher, dass er alle relevanten technischen und organisatorischen Maßnahmen so umsetzt, dass die Anforderungen der anwendbaren Gesetzgebung zum Schutz personenbezogener Daten und insbesondere der Schutz der Rechte der betroffenen Personen eingehalten werden. Vor Beginn der Verarbeitung hat der Anbieter die in **Anhang B – Technische und Organisatorische Maßnahmen (TOMs)** dieser DSA aufgeführten technischen und organisatorischen Maßnahmen eingerichtet und wird diese für die Dauer dieser DSA aufrechterhalten.

Die technischen und organisatorischen Maßnahmen hängen von der Entwicklung der Technologie ab. Der Anbieter hat das Recht, alternative angemessene Maßnahmen anzuwenden, die das gleiche oder ein höheres Maß an Sicherheit bieten.

Sobald er davon Kenntnis erlangt, jedoch nicht später als achtundvierzig (48) Stunden, informiert der Anbieter den Kunden, wenn eine Verletzung (oder potenzielle Verletzung) der persönlichen Daten des Kunden festgestellt wird. Der Anbieter stellt die ausreichenden Informationen zur Verfügung, die es dem Kunden ermöglichen, seinen Verpflichtungen zur Meldung einer Verletzung der Sicherheit personenbezogener Daten an die Aufsichtsbehörde nachzukommen. Der Anbieter erklärt, dass er Maßnahmen zur rechtzeitigen (wenn möglich sofortigen) Feststellung von Verletzungen des Schutzes personenbezogener Daten des Kunden sowie zur Rückverfolgbarkeit der Ursachen und Folgen der Verletzungen geschaffen und umgesetzt hat.

Der Anbieter ist verpflichtet, unverzüglich alle notwendigen und angemessenen Maßnahmen zu ergreifen, um die Verletzung der Sicherheit personenbezogener Daten zu beheben und mögliche nachteilige Folgen zu mindern/zu verhindern. Der Anbieter informiert den Kunden so schnell wie möglich über alle von ihm ergriffenen Maßnahmen.

Die Benachrichtigung des Anbieters über einen Sicherheitsvorfall oder die Reaktion auf einen Sicherheitsvorfall gemäß diesem Abschnitt stellt keine Anerkennung eines Fehlers oder einer Haftung des Anbieters in Bezug auf den Sicherheitsvorfall dar.

Der Kunde muss den Anbieter unverzüglich über einen möglichen Missbrauch seiner Konten oder Authentifizierungsdaten oder über Sicherheitsvorfälle im Zusammenhang mit der Dienstleistung informieren.

Benachrichtigung(en) über Sicherheitsvorfälle werden einem oder mehreren Administratoren des Kunden auf jedem vom Anbieter gewählten Weg, einschließlich per E-Mail, zugestellt. Es liegt in der alleinigen Verantwortung des Kunden, dafür zu sorgen, dass die Administratoren des Kunden bei der Anmeldung auf jedem anwendbaren Online-Service-Portal korrekte

Kontaktinformationen angeben und diese ggf. aktualisieren. Der Kunde ist allein verantwortlich für die Einhaltung seiner Verpflichtungen gemäß den für ihn geltenden Gesetzen über die Benachrichtigung bei Sicherheitsvorfällen und die Erfüllung der Benachrichtigungspflichten Dritter im Zusammenhang mit Sicherheitsvorfällen.

Der Anbieter ist verpflichtet, allfällige Datenschutzverletzungen, die den Sachverhalt der Datenschutzverletzung umfassen, so zu dokumentieren, dass der Kunde der Einhaltung der einschlägigen gesetzlichen Meldepflichten (z.B. gemäß Art. 33 und Art. 34 DSGVO) nachkommen kann.

4.5.1 Pflichten des Kunden

Der Kunde ist verpflichtet, dem Anbieter Weisungen aufgrund der Verarbeitung der Daten vor dem Datum der Annahme der Allgemeinen Geschäftsbedingungen zu erteilen.

Der Kunde ist allein dafür verantwortlich, eine unabhängige Entscheidung darüber zu treffen, ob die technischen und organisatorischen Maßnahmen für die Dienstleistung die Anforderungen des Kunden erfüllen, einschließlich seiner Sicherheitsverpflichtungen gemäß den geltenden Datenschutzanforderungen. Der Kunde erkennt an und stimmt zu, dass (unter Berücksichtigung des Standes der Technik, der Kosten der Implementierung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung seiner personenbezogenen Daten sowie der Risiken für Einzelpersonen) die vom Anbieter implementierten und aufrechterhaltenen Sicherheitspraktiken und -richtlinien ein Sicherheitsniveau bieten, das dem Risiko in Bezug auf seine personenbezogenen Daten angemessen ist. Der Kunde ist verantwortlich für die Implementierung und Aufrechterhaltung von Datenschutz- und Sicherheitsmaßnahmen für Komponenten, die er zur Verfügung stellt oder kontrolliert.

Für den Fall, dass der Kunde als Auftragsverarbeiter fungiert, garantiert der Kunde, dass die vom Kunden erteilten Weisungen von dem für die Verarbeitung jeweiligen Verantwortlichen autorisiert worden sind.

4.6 Dauer der Verarbeitung

Die Verarbeitung wird so lange fortgesetzt, wie der Anbieter Dienstleistungen aufgrund der Allgemeinen Geschäftsbedingungen für den Kunden und in Übereinstimmung mit den Weisungen des Kunden erbringt.

4.7 Rechte der betroffenen Person

Wenn sich eine betroffene Person an den Anbieter mit der Bitte wendet, ihre Rechte nach der DSGVO auszuüben, muss der Anbieter diese betroffene Person unverzüglich an den Kunden verweisen. Der Anbieter hat das Recht, die Anfrage der betroffenen Person nur nach vorheriger schriftlicher Zustimmung des Kunden zu beantworten. Der Anbieter unterstützt den Kunden bei der Bearbeitung eines angemessenen Antrags auf Ausübung der Rechte der betroffenen Person.

Der Anbieter verpflichtet sich, auf Weisung des Kunden die personenbezogenen Daten des Kunden, die sich auf die betroffene Person beziehen, unverzüglich zu berichtigen, zu löschen oder zu sperren oder jede andere vom Kunden geforderte angemessene Maßnahme durchzuführen.

4.8 Behördenanfrage

Für den Fall, dass der Kunde verpflichtet ist, einer staatlichen Behörde Informationen über die Verarbeitung personenbezogener Daten des Kunden zu erteilen oder anderweitig mit dieser Behörde zusammenzuarbeiten, ist der Anbieter verpflichtet, den Kunden bei der Erteilung dieser Informationen zu unterstützen, indem er bei der unverzüglichen Bereitstellung der entsprechenden Informationen oder Unterlagen behilflich ist, dazu gehören die ergriffenen technischen und organisatorischen Maßnahmen, die Orte, an denen die personenbezogenen Daten des Kunden verarbeitet werden, und die an der Verarbeitung beteiligten Personen.

5 Datenübertragung und Standort

5.1 Datenübertragung

Die Datenverarbeitungstätigkeiten werden auf dem Hoheitsgebiet eines Mitgliedstaates der Europäischen Union (EU) oder eines anderen Mitgliedstaates des Abkommens über den Europäischen Wirtschaftsraum (EWR) durchgeführt. Eine Datenverarbeitung in einen Staat außerhalb der EU darf nur erfolgen, wenn die besonderen Bedingungen des Kapitels V des DSGVO erfüllt sind.

5.2 Unterauftragsverarbeiter

Für den Fall, dass der Anbieter Unterauftragsverarbeiter einsetzt, die Daten übertragen könnten, akzeptiert der Kunde die Geschäftsbedingungen des jeweiligen Unterauftragsverarbeiters bezüglich der Datenübertragung.

6 Aufbewahrung und Löschen von Daten

Der Kunde hat während der Laufzeit seines Abonnements jederzeit die Möglichkeit, auf die gespeicherten Kundendaten zuzugreifen, sie zu extrahieren und zu löschen. Nach Beendigung der Erbringung der Dienstleistung ist der Anbieter verpflichtet, nach Ermessen des Kunden alle vom Kunden zur Verfügung gestellten personenbezogenen Daten und alle zusätzlich erworbenen personenbezogenen Daten des Kunden einschließlich aller Kopien vollständig und unwiderruflich zurückzugeben und zu löschen, sofern und soweit nicht die Ausnahme nach Art. 28 Ziff. 3 lit. l. "g" der DSGVO anwendbar ist.

Der Anbieter erstellt ein Dokument für die Löschung der persönlichen Daten des Kunden und stellt es dem Kunden zur Verfügung. Der Kunde kann zu diesem Zeitpunkt oder zu einem späteren Zeitpunkt die Herausgabe der entsprechenden Protokolldateien verlangen.

Die Dokumentation, die dem Nachweis der Übereinstimmung der Verarbeitung der persönlichen Daten des Kunden mit der erbrachten Dienstleistung und den Verarbeitungsregeln dient, wird vom Anbieter nach Beendigung der Leistungserbringung gemäß den entsprechenden Aufbewahrungsfristen aufbewahrt.

7 Vertraulichkeitsverpflichtung des Datenverarbeiters

Der Anbieter stellt sicher, dass seine Mitarbeiter, die mit der Verarbeitung von Kundendaten und personenbezogenen Daten befasst sind, diese Daten nur auf Weisung des Kunden oder wie in dieser DSA beschrieben verarbeiten, und verpflichtet sind, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung des Auftrags zu wahren. Der Anbieter bietet seinen Mitarbeitern, die Zugang zu Kundendaten und personenbezogenen Daten haben, gemäß den geltenden Datenschutzanforderungen und Industriestandards regelmäßige und obligatorische

Datenschutz- und Sicherheitsschulungen sowie Sensibilisierungsmaßnahmen an.

8 Einsatz von Unterauftragsverarbeitern

Der Anbieter kann Unterauftragsverarbeiter damit beauftragen, bestimmte beschränkte oder zusätzliche Dienstleistungen in seinem Namen zu erbringen. Der Kunde stimmt dieser Beauftragung und den mit dem Anbieter verbundenen Unternehmen als Unterauftragsverarbeiter zu, indem er die Allgemeinen Geschäftsbedingungen des Anbieters akzeptiert.

Der Anbieter stellt Informationen über Unterauftragsverarbeiter auf einer Website des Anbieters zur Verfügung. Mit der Annahme der Allgemeinen Geschäftsbedingungen des Anbieters erklärt der Kunde, dass er die jeweiligen Datenschutzbestimmungen der Unterauftragsverarbeiter gelesen, verstanden und akzeptiert hat. Bei der Beauftragung eines Unterauftragsverarbeiters stellt der Anbieter sicher, dass der Unterauftragsverarbeiter nur auf Kundendaten oder persönliche Daten zugreifen und diese nur für die Erbringung der Dienstleistungen verwenden darf, für die der Anbieter sie aufbewahrt hat, und dass es ihm untersagt ist, Kundendaten oder persönliche Daten für andere Zwecke zu verwenden. Der Anbieter ist verpflichtet, die Einhaltung der Verpflichtungen mindestens einmal pro Jahr zu überprüfen.

9 Allgemeine Bedingungen

9.1 Begrenzte Updates / Änderungen der DSA-Bedingungen

Wenn der Kunde ein neues Abonnement für einen vom Anbieter bereitgestellten Dienst erneuert oder erwirbt, gelten die dann aktuellen DSA-Bedingungen und ändern sich während des Abonnements des Kunden für diese Dienstleistung nicht. Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen kann der Anbieter, wenn er neue Funktionen, Ergänzungen oder zugehörige Software einführt, zusätzliche Bedingungen bereitstellen oder Aktualisierungen der DSA vornehmen, die für die Nutzung dieser durch den Kunden gelten.

Für den Fall, dass diese Bedingungen wesentliche nachteilige Änderungen an den DSA-Bedingungen enthalten, wird der Anbieter dem Kunden die Wahl lassen, die neuen Funktionen, Ergänzungen oder zugehörige Software zu nutzen, ohne die bestehende Funktionalität eines allgemein verfügbaren Dienstes zu verlieren. Wenn der Kunde die neuen Funktionen, Ergänzungen oder die zugehörige Software nicht nutzt, gelten die entsprechenden neuen Bedingungen nicht.

9.2 Gesetzliche Vorschriften und Anforderungen

Ungeachtet der vorstehenden Beschränkungen für Aktualisierungen kann der Anbieter eine Dienstleistung in jedem Land oder jeder Gerichtsbarkeit modifizieren oder beenden, in dem eine gegenwärtige oder zukünftige behördliche Anforderung oder Verpflichtung besteht, die den Anbieter einer Regelung oder Anforderung unterwirft, die nicht allgemein auf dort tätige Unternehmen anwendbar ist, die für den Anbieter eine Härte darstellt, den Online-Service ohne Änderung weiter zu betreiben und/oder die den Anbieter zu der Annahme veranlasst, dass die DSA-Bedingungen oder die bereitgestellte Dienstleistung im Widerspruch zu einer solchen Anforderung oder Verpflichtung stehen könnten.

9.3 Elektronische Benachrichtigung

Der Anbieter kann dem Kunden Informationen und Mitteilungen über den Service elektronisch, auch per E-Mail, auf eine Weise zukommen lassen, die den Anbieter identifiziert. Benachrichtigungen gelten als an dem Tag erfolgt, an dem sie durch den Anbieter bereitgestellt werden.

9.4 Kontaktdaten des Anbieters

Der Kunde kann sich an den Kundensupport des Anbieters wenden unter:

support24@gbs.com

+49 69 808 852 88 (Hotline DE/EN 24/7/365)

1 Anhang A – Arten der verarbeiteten Daten des Kunden

Dieser Anhang enthält Einzelheiten über die Verarbeitung von personenbezogenen Daten gemäß Art. 28 Abs. 3 DSGVO.

1.1 **Arten von personenbezogenen Daten:**

- Name;
- PIN;
- Telefonnummer;
- Adresse;
- usw.

1.2 Aktivitäten der **Datenverarbeitung**:

- Sammeln;
- Aufzeichnen;
- Speichern;
- Weiterleiten;
- Posten;
- Löschen;
- Vernichten.

1.3 **Zweck der Verarbeitung:**

- Sichere Kundenkommunikation;
- Suche nach schädlichem Inhalt;
- Einhaltung der gesetzlichen Bestimmungen durch Hinzufügen von Ausschlussklauseln;
- Verbesserung der Produktivität durch Abwesenheitsfunktionalitäten.

1.4 **Kategorien der betroffenen Personen:**

- Angestellte;
- Kunden;
- Vertragspartner;
- Website Besucher.

1 Anhang B – Technische und Organisatorische Maßnahmen (TOMs)

1.1 Organisatorische Sicherheitsmaßnahmen

1.1.1 Sicherheits-Management

a. Sicherheitspolitik und -verfahren: Der Anbieter muss eine Sicherheitspolitik in Bezug auf die Verarbeitung personenbezogener Daten dokumentieren.

b. Rollen und Verantwortlichkeiten:

i. Die Rollen und Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten sind klar definiert und gemäß der Sicherheitspolitik zugewiesen;

ii. Bei internen Umstrukturierungen oder Kündigungen und Wechsel des Arbeitsverhältnisses ist der Widerruf von Rechten und Pflichten mit entsprechenden Übergabeverfahren klar definiert.

c. Zugangskontrollpolitik: Jeder Rolle, die an der Verarbeitung personenbezogener Daten beteiligt ist, werden nach dem Need-to-know-Prinzip spezifische Zugriffskontrollrechte zugewiesen.

d. Resourcen-/Vermögens-Management: Der Anbieter verfügt über ein Register der IT-Ressourcen, die für die Verarbeitung personenbezogener Daten verwendet werden (Hardware, Software und Netzwerk). Mit der Pflege und Aktualisierung des Registers ist eine bestimmte Person beauftragt (z.B. IT-Beauftragter).

e. Änderungs-Management: Der Anbieter stellt sicher, dass alle Änderungen am IT-System von einer bestimmten Person (z.B. IT- oder Sicherheitsbeauftragter) registriert und überwacht werden. Dieser Prozess wird regelmäßig überwacht.

1.1.2 Reaktion auf Vorfälle und Geschäftskontinuität

a. Behandlung von Vorfällen / Verletzungen von personenbezogenen Daten:

i. Es wird ein Vorfallreaktionsplan mit detaillierten Verfahren festgelegt, um eine wirksame und geordnete Reaktion auf Vorfälle im Zusammenhang mit personenbezogenen Daten zu gewährleisten.

ii. Der Anbieter wird dem Kunden unverzüglich jeden Sicherheitsvorfall melden, der zu einem Verlust, Missbrauch oder unbefugtem Erwerb von personenbezogenen Daten geführt hat.

b. Geschäftskontinuität: Der Anbieter legt die wichtigsten Verfahren und Kontrollen fest, die zu befolgen sind, um das erforderliche Maß an Kontinuität und Verfügbarkeit des IT-Systems zu gewährleisten, in dem personenbezogene Daten verarbeitet werden (im Falle eines Vorfalls/einer Verletzung der personenbezogenen Daten).

1.2 Personalwesen

a. Vertraulichkeit der Mitarbeiter: Der Anbieter stellt sicher, dass alle Mitarbeiter hinreichend informiert sind und ihre Verantwortlichkeiten und Verpflichtungen im Zusammenhang mit der Verarbeitung personenbezogener Daten verstehen. Rollen und Verantwortlichkeiten werden während des Voreinstellungs- und/oder Einarbeitungsprozesses klar kommuniziert.

b. Training: Der Anbieter stellt sicher, dass alle Mitarbeiter angemessen über die Sicherheitskontrollen des IT-Systems informiert sind, die sich auf ihre tägliche Arbeit beziehen. Mitarbeiter, die mit der Verarbeitung personenbezogener Daten befasst sind, werden auch durch regelmäßige Sensibilisierungskampagnen über die einschlägigen Datenschutzvorschriften und rechtlichen Verpflichtungen angemessen informiert.

2 Technische Sicherheitsmaßnahmen

2.1 Pseudonymisierung

Die Mitarbeiter der Kunden sind dazu angehalten, Supportanfragen mit simulierten/anonymisierten Daten zu übermitteln - personenbezogene Daten Dritter sind in der Regel nicht vorhanden oder werden gelöscht.

2.2 Verschlüsselung

Durchgängige Laufwerksverschlüsselung an Kunden und Server, Verschlüsselung aller Datenbanken (Server- und Kundenseitig), Verschlüsselungstechnologien für VPN-Verbindungen.

2.3 Zugriffsskontrolle und Authenifizierung

a. Es wird ein Zugriffskontrollsystem implementiert, das für alle Benutzer gilt, die auf das IT-System zugreifen. Das System ermöglicht das Erstellen, Genehmigen, Überprüfen und Löschen von Benutzerkonten.

b. Die Verwendung von gemeinsamen Benutzerkonten wird vermieden. In Fällen, in denen dies erforderlich ist, wird sichergestellt, dass alle Benutzer des gemeinsamen Kontos die gleichen Rollen und Verantwortlichkeiten haben.

c. Bei der Gewährung des Zugriffs oder der Zuweisung von Benutzerrollen ist das "Need-to-know-Prinzip" zu beachten, um die Anzahl der Benutzer, die Zugriff auf personenbezogene Daten haben, auf diejenigen zu beschränken, die sie zur Erreichung der Verarbeitungszwecke des Anbieters benötigen.

d. Wenn die Authentifizierungsmechanismen auf Passwörtern basieren, verlangt der Anbieter, dass das Passwort mindestens acht Zeichen lang ist und sehr starken Passwortkontrollparametern wie Länge, Zeichenkomplexität und Nicht-Wiederholbarkeit entspricht.

e. Die Authentifizierungs-Zugangsdaten (wie Benutzer-ID und Passwort) dürfen niemals ungeschützt über das Netzwerk übertragen werden.

2.4 Protokollierung und Überwachung:

Protokolldateien werden für jedes System/jede Anwendung aktiviert, das/die für die Verarbeitung personenbezogener Daten verwendet wird. Sie umfassen alle Arten des Zugriffs auf Daten (Anzeigen, Ändern, Löschen).

2.5 **Sicherheit der Daten im Ruhezustand**

2.5.1 **Server-/Datenbank-Sicherheit**

i. Datenbank- und Anwendungsserver sind so konfiguriert, dass sie unter Verwendung eines separaten Kontos mit minimalen Betriebssystemprivilegien laufen, damit sie korrekt funktionieren.

ii. Datenbank- und Anwendungsserver verarbeiten nur die personenbezogenen Daten, die zur Erreichung ihrer Verarbeitungszwecke tatsächlich benötigt werden.

2.5.2 **Sicherheit am Arbeitsplatz:**

i. Benutzer sind nicht in der Lage, Sicherheitseinstellungen zu deaktivieren oder zu umgehen.

ii. Antiviren-Anwendungen und Virendefinitionen werden kontinuierlich aktualisiert.

iii. Benutzer haben nicht die Berechtigung, nicht autorisierte Software-Anwendungen zu installieren oder zu aktivieren.

iv. Das System verfügt über Sitzungszeitüberschreitungen, wenn der Benutzer eine bestimmte Zeit lang nicht aktiv war.

v. Kritische Sicherheitsupdates, die vom Entwickler des Betriebssystems veröffentlicht werden, werden regelmäßig installiert.

2.6 **Netzwerk-/Kommunikations-Sicherheit:**

a. Wann immer der Zugriff über das Internet erfolgt, wird die Kommunikation durch kryptographische Protokolle verschlüsselt.

b. Der Verkehr zum und vom IT-System wird durch Firewalls und Intrusion Detection Systems überwacht und gesteuert.

2.7 **Back-ups:**

a. Backup- und Datenwiederherstellungsverfahren sind definiert, dokumentiert und klar mit Rollen und Verantwortlichkeiten verknüpft.

b. Backups erhalten ein angemessenes Maß an physischem und ökologischem Schutz, das den auf die Ursprungsdaten angewandten Standards entspricht.

c. Die Ausführung der Backups wird auf Vollständigkeit überwacht.

2.8 **Mobile/tragbare Geräte:**

a. Es werden Verfahren zur Verwaltung mobiler und tragbarer Geräte definiert und dokumentiert, die klare Regeln für ihre ordnungsgemäße Verwendung festlegen.

b. Mobile Geräte, die auf das Informationssystem zugreifen dürfen, sind vorregistriert und vorautorisiert.

2.9 Sicherheit im Lebenszyklus von Anwendungen:

Während des gesamten Entwicklungslebenszyklus werden bewährte Verfahren, der Stand der Technik und anerkannte sichere Entwicklungspraktiken oder -standards befolgt.

2.10 **Löschen und Vernichten von Daten:**

a. Softwarebasiertes Überschreiben wird auf Medien vor ihrer Entsorgung durchgeführt. In Fällen, in denen dies nicht möglich ist (CD's, DVD's usw.), wird eine physische Zerstörung durchgeführt.

b. Papier und tragbare Datenträger, die zur Speicherung persönlicher Daten verwendet werden, werden vernichtet.

2.11 **Physische Sicherheit**

Der physische Perimeter

der IT-Systeminfrastruktur ist für nicht autorisiertes Personal nicht zugänglich. Es sind geeignete technische Maßnahmen (z.B. Intrusion Detection System, chipkartengesteuertes Drehkreuz, Ein-Personen-Sicherheitszugangssystem, Schließanlage) oder organisatorische Maßnahmen (z.B. Sicherheitswache) zu treffen, um Sicherheitsbereiche und deren Zugänge vor dem Zutritt Unbefugter zu schützen.