# Verpflichtungserklärung

zur Einhaltung
des **Datengeheimnisses** und der **Datensicherheit**

## 1. Einleitung

Diese Erklärung beinhaltet die auf Grundlage der Norm ISO 27001 zur Informationssicherheit abzuschließende Verpflichtungserklärung des Auftraggebers zur Einhaltung des Datengeheimnisses und der Datensicherheit durch den Auftragnehmer.

## 2. Gegenstand der Erklärung

(1) Gegenstand der Erklärung ist die Durchführung eines Auftrages durch den Auftragnehmer. Diese Erklärung ist als Ergänzung zu der Bestellung/Hauptvertrag zu sehen.

(2) Im Zuge dieser Tätigkeit kann der Auftragnehmer Kenntnis über – auch nicht personenbezogene - **interne Informationen des Auftraggebers**, dessen Kunden oder Geschäftspartner sowie über dessen Mitarbeiter erlangen. Interne Informationen sind vor allem Dokumente und Unterlagen betreffend kaufmännischer und rechtlicher Angelegenheiten, Betriebsgeheimnissen und technischem Wissen, die dem Auftragnehmer direkt oder indirekt im Zuge seiner Tätigkeit für den Auftraggeber zugänglich werden. Dies betrifft sowohl Informationen in elektronischer, schriftlicher, aber auch mündlicher Form, gleichgültig ob sie als intern, vertraulich oder Ähnliches gekennzeichnet oder nur vom Inhalt her als firmenintern erkennbar sind.

(3) Der Auftragnehmer ist verpflichtet, die im Zusammenhang mit seiner Tätigkeit erworbenen internen Informationen als **Geschäftsgeheimnis** zu behandeln, sie ohne ausdrückliche schriftliche Zustimmung des Auftraggebers weder offenzulegen, noch zu veröffentlichen, kommerziell zu verwenden oder Unbefugten –die nicht vom Auftraggeber mit dem Auftrag betraut wurden- zu überlassen oder auf sonstige Art und Weise zugänglich zu machen. Diese Geheimhaltungspflicht bleibt auch nach Beendigung des Auftrags für den Auftragnehmer aufrecht.

(4) Der Auftragnehmer hat sämtliche Informationen, die ihm zur Umsetzung des Auftrages übergeben wurden, unabhängig von deren Form (in Papier oder elektronischer Form) nach dem **Stand der Technik zu schützen** und alle erforderlichen Informationssicherheitsmaßnahmen zu treffen.

(5) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Dafür müssen alle befugten Dienstnehmer des Auftragnehmers die **Anlage ./1 „verpflichtende Information an die befugten Dienstnehmer des Auftragnehmers“** gelesen haben. Dadurch erhalten diese Dienstnehmer Kenntnis der gegenständlichen Verpflichtungsvereinbarung und verpflichten sich zur Einhaltung dieser. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(6) Für den Fall, dass sich der Auftragnehmer **Erfüllungsgehilfen** bedient, verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber, dass diesen Erfüllungsgehilfen vor Offenlegung von Informationen ebenfalls die Anlage ./1 „verpflichtende Information an die befugten Dienstnehmer des Auftragnehmers“ vorgelegt wird. Dabei sind unter dem Begriff „Dienstnehmer“ auch alle anderen Erfüllungsgehilfen des Auftragnehmers zu verstehen.
Der Auftragnehmer garantiert die Einhaltung der Bestimmungen dieser Vereinbarung durch diese Erfüllungsgehilfen.

(7) Der Auftragnehmer ist befugt Unternehmen als Sub-Auftragnehmer hinzuzuziehen:
Eine aktuelle Liste aller Sub-Auftragnehmer ist dem Auftraggeber vor Auftragsbeginn schriftlich bekannt zu geben. Beabsichtigte Änderungen des Sub-Auftragnehmers sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Vom Auftragnehmer ist sicherzustellen, dass der Sub-Auftragnehmer dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung

obliegen. Kommt der Sub-Auftragnehmer seinen Pflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragnehmers.

(8) Das Anfertigen von Aufzeichnungen, Abschriften oder Kopien von internen Informationen, insbesondere von geschäftlichen Unterlagen sowie das Entfernen von Geschäftspapier und -unterlagen aus den Räumlichkeiten des Auftraggebers für Zwecke, die keinen Zusammenhang mit dem Auftrag aufweisen, ist dem Auftragnehmer ohne vorherige Zustimmung des Auftraggebers streng untersagt. Mitgenommene Geschäftspapiere und –unterlagen bleiben im **Eigentum** des Auftraggebers. Sie dürfen Unbefugten nicht überlassen werden und müssen so aufbewahrt werden, dass die Einhaltung dieser Vereinbarung gewährleistet ist.

(9) Nach Beendigung der Laufzeit oder Kündigung des Auftrages sind sämtliche Verarbeitungsergebnisse und Unterlagen, die Informationen des Auftraggebers enthalten, diesem zu übergeben (oder allenfalls in seinem Auftrag für ihn weiter aufzubewahren) oder nicht länger als gesetzlich unbedingt erforderlich aufzubewahren und sodann zu **vernichten bzw. zu löschen**.

(10) **Ausnahmen** der Geheimhaltung:
Von der Geheimhaltungspflicht ausgenommen sind Informationen,

(i) die bereits öffentlich bekannt sind;
(ii) die der Auftragnehmer bzw. seine Dienstnehmer unabhängig vom Auftrag rechtmäßig, insbesondere nicht durch Verletzung von Verschwiegenheitsverpflichtungen des Informationsgebers erlangt haben;
(iii) die gegenüber Behörden oder Parteien, insbesondere im Zuge eines Verfahrens zur Erlangung einer behördlichen Bewilligung, offenzulegen sind sowie
(iv) Informationen, die in einem Verwaltungsverfahren, straf- bzw. zivilgerichtlichen Verfahren aufgrund richterlichen Auftrags (Verfügung) bekannt gegeben werden müssen (ohne dass diese von einem Entschlagungsrecht umfasst sind).

Im Fall von (iii) und (iv) ist der Auftraggeber zur Wahrung seiner Interessen unverzüglich von der Bekanntgabe der Informationen zu unterrichten.

## 3. Einhaltung technischer und organisatorischer Maßnahmen und Datenschutz

(1) Der Auftragnehmer erklärt rechtsverbindlich, dass er die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Informationen des Auftraggebers setzt. Der Auftragnehmer garantiert dabei, dass er zumindest die meisten der in Anlage ./2 angeführten Maßnahmen setzt und dem Auftraggeber eine genau Auflistung aller Maßnahmen zeitnah nach Auftragserteilung unaufgefordert zukommen lässt.

(2) Grundsätzlich werden bei der Erfüllung dieses Auftrages **keine personenbezogenen Daten** im Sinne der nationalen und internationalen Datenschutzvorschriften verarbeitet. Soweit aber doch während Erfüllung des Auftrages personenbezogene Daten verarbeitet werden, verpflichtet sich der Auftragnehmer umgehend den Auftraggeber darüber zu informieren und gegebenenfalls eine Vereinbarung einer Auftragsverarbeitung gemäß Art 28 DSGVO abzuschließen.

(3) Ist der Abschluss einer Vereinbarung einer Auftragsverarbeitung gemäß Art 28 DSGVO erforderlich, so ersetzt diese Vereinbarung einer Auftragsvereinbarung die gegenständliche Verpflichtungserklärung.

## 4. Sonstiges

(4) Diese Verpflichtungserklärung unterliegt **österreichischem Recht**. Zur Entscheidung aller aus dieser Erklärung entstehenden Streitigkeiten wird das sachlich in Betracht kommende Gericht in Bregenz vereinbart.

(5) Änderungen oder Ergänzungen dieser Verpflichtungserklärung bedürfen zu ihrer Wirksamkeit der **Schriftform**. Soweit im Auftrag Regelungen zu Datengeheimnis und Datensicherheit festgelegt wurden, gehen diese Regelungen jenen der Verpflichtungserklärung vor. Soweit die Regelungen dieser Verpflichtungserklärung jedoch die Regelungen des Auftrages lediglich konkretisieren bzw. ergänzen und kein Widerspruch zwischen beiden vorliegt, gelten die Regelungen nebeneinander.

(6) Sollte eine Bestimmung dieser Verpflichtungserklärung ganz oder teilweise unwirksam oder undurchführbar sein, beeinträchtigt dies die Wirksamkeit oder Durchführbarkeit der übrigen Bestimmungen nicht. Die unwirksame oder undurchführbare Bestimmung wird durch eine wirksame oder durchführbare Bestimmung ersetzt, die in ihrem wirtschaftlichen Gehalt und in ihrem Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung möglichst nahekommt; dasselbe gilt entsprechend im Falle allfälliger Lücken in dieser Verpflichtungserklärung (**Salvatorische Klausel**).

(7) Durch den Abschluss des Hauptvertrages bestätigt der Auftragnehmer diese Erklärung **zustimmend zur Kenntnis** genommen zu haben

Anlage 1: verpflichtende Information an die befugten Dienstnehmer
Anlage ./2 ¬– Technisch-organisatorische Maßnahmen

# Anlage ./1 – verpflichtende Information an die befugten Dienstnehmer des Auftragnehmers

Anlage zur Vereinbarung zur Einhaltung des **Datengeheimnisses, der Datensicherheit und des Datenschutzes** gemäß den geltenden nationalen und internationalen Datenschutzvorschriften sowie der Verschwiegenheit betreffend interner Informationen.

## 1. Allgemein

1.1. Diese verpflichtende Information wird durch den Auftragnehmer allen mit der Datenverarbeitung beauftragten Personen (Dienstnehmer) vor Aufnahme der Tätigkeit vorgelegt. Alle befugten Dienstnehmer des Auftragnehmers müssen diese Information gelesen haben. Eine Kopie dieser Information ist dem Dienstnehmer zu übergeben.

1.2. Durch diese Information erhalten die Dienstnehmer Kenntnis der gegenständlichen Verpflichtungsvereinbarung und verpflichten sich zur Einhaltung dieser. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

1.3. Der Dienstnehmer wurde über die von seinem Dienstgeber unterfertigte Vereinbarung zur Einhaltung des Datengeheimnisses, der Datensicherheit und des Datenschutzes vollinhaltlich in Kenntnis gesetzt.

1.4. Die Verpflichtungen aus dieser Information gelten auch nach Beendigung der Tätigkeit für den Auftraggeber oder mit ihm verbundener Unternehmen bzw. nach Auflösung des jeweiligen Dienstverhältnisses.

## 2. Pflichten des Dienstnehmers

2.1. Der Dienstnehmer muss die einschlägigen gesetzlichen nationalen und internationalen **Datenschutzvorschriften** in der jeweils gültigen Fassung einhalten.

2.2. Jede **nicht auftragsgemäße Verarbeitung** von im Rahmen seiner Tätigkeit für den Auftraggeber oder mit ihm verbundenen Unternehmen erhaltenen Informationen, Zugangs- und Zugriffsberechtigungen ist dem Dienstnehmer **untersagt.** Darunter fällt auch die nicht autorisierte Weitergabe von Zugangs-oder Zugriffsberechtigungen innerhalb des Unternehmens des Auftragnehmers.

2.3. Die **Nutzung der IT Infrastruktur** des Auftraggebers ist nur für den geschäftlichen Gebrauch im Rahmen des Auftrages gestattet. Die Hardware und Software dürfen nur bestimmungsgemäß eingesetzt werden. Die Nutzung externer Datenträger ist untersagt. Die Inbetriebnahme von eigener Hardware oder Software im Datennetz des Auftraggebers ist untersagt, sofern nicht vom Auftraggeber ausdrücklich erlaubt.

2.4. Arbeiten an **IT-Systemen** des Auftraggebers sind mit dem Auftraggeber jeweils vorab einvernehmlich festzulegen, andernfalls der Einsatz der Hardware oder der Software nicht als bestimmungsgemäß bzw. als für den geschäftlichen Gebrauch gestattet angesehen wird und der Auftragsnehmer für den allenfalls eingetretenen Schaden zu haften hat.

2.5. **Passwörter** sind geheim zu halten und dürfen weder schriftlich noch mündlich weitergegeben werden.

2.6. Der Dienstnehmer muss von einem vom Auftraggeber für ihn nominierten Betreuer bei Bedarf in die **Räumlichkeiten** des Auftraggebers eingeführt werden. Der Dienstnehmer darf die Räumlichkeiten nur innerhalb der Bürozeiten des Auftraggebers und nur durch den Haupteingang betreten und verlassen und muss auf direktem Weg seinen ihm zugewiesenen Arbeitsplatz aufsuchen und sämtliche sonstigen Ausgänge geschlossen halten.

2.7. Jedes Betreten und Verlassen der Räumlichkeiten ist aus Sicherheitsgründen an den **Zugangskontrollen** ordnungsgemäß zu verbuchen (soweit an der betreffenden Örtlichkeit vorgesehen, wird eine Zutrittskarte vom Verantwortlichen (z.B. Projektleiter Auftraggeber) organisiert bzw. ist als Besucherkarte beim Portier abzuholen).

2.8. Ist der Dienstnehmer in der Funktion eines **System- oder Netzwerkadministrators** tätig, kann die Situation entstehen, dass er aufgrund planmäßiger Arbeiten an Systemen oder Netzwerken bzw. im Rahmen von Fehleranalysen an Servern, Clients oder Netzwerkkomponenten Kenntnis von Inhaltsdaten erlangt. Dem Erklärenden ist bewusst, dass er derartige Informationen keinesfalls weitergeben oder auf andere Weise verwenden darf. Außerdem ist dem Erklärenden ausdrücklich untersagt, sich unberechtigten Zugang zu Systemen, Daten oder Informationen zu verschaffen.
Der zuständige Administrator des Auftraggebers übergibt an den Dienstnehmer des Auftragnehmers die Administrationsrichtlinie mit den detaillierten Vorgaben für Arbeiten beim Auftraggeber. Diese Richtlinie ist integraler Bestandteil der vorliegenden Verpflichtungserklärung.

2.9. **Remote-Wartungsaktivitäten** dürfen ausschließlich von Arbeitsgeräten aus erfolgen, die eine aktuelle Antivirensoftware installiert haben und die einen aktuellen sicherheitstechnischen Patch-Level aufweisen und nur via der zentralen vom Auftraggeber vorgesehenen Remote Access Lösung. Weiters wird der Dienstnehmer hiermit darüber informiert, dass sämtliche Remote-Zugriffe protokolliert werden.

## 3. Rechte des Auftraggebers

Der Auftraggeber kann zum Schutz seines Eigentums und der Mitarbeiter per **Video überwachte** Bereiche haben. Der Dienstnehmer wird hiermit über eine solche Videoüberwachung informiert.
Bei Fragen zu der Videoüberwachung kann sich der Dienstnehmer an den Auftraggeber wenden.

# Anlage ./2 – Technisch-organisatorische Maßnahmen

**Vertraulichkeit**

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten;
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (streng vertraulich/vertraulich/intern/öffentlich).

**Integrität**

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumenten-management;

**Verfügbarkeit und Belastbarkeit**

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/ Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragnehmers (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.