Informationssicherheitserklärung

I. Einleitung

Diese Erklärung beinhaltet die auf Grundlage der Norm ISO 27001 zur Informationssicherheit abzuschließende Erklärung zur Einhaltung der erforderlichen Vertraulichkeit und technischer und organisatorischer Maßnahmen.

II. Gegenstand der Erklärung

1. Gegenstand der Erklärung ist die Durchführung eines Auftrages durch den Auftragnehmer. Diese Erklärung gilt als ergänzender Bestandteil der Bestellung bzw. des Hauptvertrages.
2. Im Zuge dieser Tätigkeit kann der Auftragnehmer Kenntnis von internen Informationen – auch von nicht personenbezogenen Informationen – des Auftraggebers, dessen Kunden oder Geschäftspartner sowie dessen Mitarbeitern erlangen. Interne Informationen sind vor allem Dokumente und Unterlagen betreffend kaufmännische und rechtliche Angelegenheiten, Betriebsgeheimnisse und technisches 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 Informationsverarbeitung 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 Informationssicherheitserklärung und verpflichten sich zur Einhaltung dieser. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Informationsverarbeitung 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 Erklärung durch diese Erfüllungsgehilfen.

Der Auftragnehmer darf Sub-Auftragnehmer nur nach vorheriger schriftlicher Bekanntgabe dieser an den Auftraggeber hinzuziehen. 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 Erklärung obliegen. Kommt der Sub-Auftragnehmer seinen Pflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragnehmers.

7. Das Anfertigen von Aufzeichnungen, Abschriften oder Kopien von internen Informationen, insbesondere von geschäftlichen Unterlagen sowie das Entfernen von Geschäftspapieren 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 Erklärung gewährleistet ist.

8. 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**. Auf Verlangen des Auftraggebers ist über die Löschung eine schriftliche Bestätigung auszuhändigen.

9. **Ausnahmen** der Geheimhaltung:

   Von der Geheimhaltungspflicht ausgenommen sind Informationen,

   9.1. die bereits öffentlich bekannt sind;

   9.2. die der Auftragnehmer bzw. seine Dienstnehmer unabhängig vom Auftrag rechtmäßig, insbesondere nicht durch Verletzung von Verschwiegenheitsverpflichtungen des Informationsgebers erlangt haben;

   9.3. die gegenüber Behörden oder Parteien, insbesondere im Zuge eines Verfahrens zur Erlangung einer behördlichen Bewilligung, offenzulegen sind sowie

   9.4. die in einem Verwaltungsverfahren, straf- bzw. zivilgerichtlichen Verfahren aufgrund richterlichen Auftrags (Verfügung) gegenüber Behörden und Gerichten bekannt gegeben werden müssen (ohne dass diese von einem Entschlagungsrecht umfasst sind).

   Im Fall von 9.3 und 9.4 ist der Auftraggeber zur Wahrung seiner Interessen unverzüglich von der Bekanntgabe der Informationen zu unterrichten.

III. Einhaltung technischer und organisatorischer Maßnahmen

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 in Anlage ./2 angeführten Maßnahmen erfüllt und dem Auftraggeber eine genaue Auflistung aller Maßnahmen zeitnah nach Auftragserteilung unaufgefordert zukommen lässt.

Grundsätzlich werden bei der Erfüllung dieses Auftrages keine personenbezogenen Daten im Sinne der nationalen und internationalen Datenschutzvorschriften verarbeitet. Soweit im Rahmen der Erfüllung des Auftrages personenbezogene Daten verarbeitet werden, verpflichtet sich der Auftragnehmer, den Auftraggeber vor Beginn der Verarbeitung darüber zu informieren und erforderlichenfalls eine Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO abzuschließen.

IV. Sonstiges

1. Diese Informationssicherheitserklärung unterliegt **österreichischem Recht**. Zur Entscheidung aller aus dieser Erklärung entstehenden Streitigkeiten wird das sachlich in Betracht kommende Gericht in Bregenz vereinbart.
2. Änderungen oder Ergänzungen dieser Informationssicherheitserklärung bedürfen zu ihrer Wirksamkeit der **Schriftform**. Soweit im Auftrag spezifische Regelungen zu Vertraulichkeit sowie technischen und organisatorischen Maßnahmen festgelegt wurden, gehen diese Regelungen den Bestimmungen dieser Informationssicherheitserklärung nur insoweit vor, als sie den Schutzstandard dieser Informationssicherheitserklärung nicht unterschreiten oder ausdrücklich eine abweichende Regelung vereinbart wurde. Soweit die Regelungen dieser Informationssicherheitserklärung jedoch die Regelungen des Auftrages lediglich konkretisieren bzw. ergänzen und kein Widerspruch zwischen beiden vorliegt, gelten die Regelungen nebeneinander.
3. Sollte eine Bestimmung dieser Informationssicherheitserklärung 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 Informationssicherheitserklärung (**Salvatorische Klausel**).
4. Durch die Annahme des Auftrags bestätigt der Auftragnehmer, dass ihm diese Erklärung zugänglich war, er die Möglichkeit zur Kenntnisnahme hatte und deren Geltung akzeptiert.

Beilage:

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

Anlage ./2: Technisch-organisatorische Maßnahmen

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

Anlage zur Informationssicherheitserklärung.

1. Allgemein

1.1. Diese verpflichtende Information wird durch den Auftragnehmer allen mit der Informationsverarbeitung 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 Informationssicherheitserklärung und verpflichten sich zur Einhaltung dieser. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Informationsverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

1.3. Der Dienstnehmer wurde über die Informationssicherheitserklärung 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.

2. Pflichten des Dienstnehmers

2.1. 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.

2.2. 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.

2.3. 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 Auftragnehmer für den allenfalls eingetretenen Schaden zu haften hat.

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

2.5. 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 Betriebs-/Bürozeiten des Auftraggebers und nur durch den vorgesehenen Eingang betreten und verlassen und muss auf direktem Weg seinen ihm zugewiesenen Arbeitsplatz aufsuchen und sämtliche sonstigen Ausgänge geschlossen halten. Abweichende Vorgehensweisen dürfen nur mit Zustimmung des Auftraggebers erfolgen.

2.6. 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).

2.7. 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 Informationssicherheitserklärung.

2.8. Remote-Wartungsaktivitäten dürfen ausschließlich von Arbeitsgeräten aus erfolgen, die eine aktuelle Endpunktsicherheitslösung installiert haben und die einen aktuellen sicherheitstechnischen Patch-Level aufweisen. Der Zugang ist nur über die zentralen vom Auftraggeber vorgesehenen Remote-Access-Lösung erlaubt. 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 videoüberwachte 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

Der Auftragnehmer garantiert, dass er zumindest folgende angeführten Maßnahmen setzt und dem Auftraggeber eine genau Auflistung aller Maßnahmen zeitnah nach Auftragserteilung unaufgefordert zukommen lässt:

Vertraulichkeit

- **Zutrittskontrolle**: Schutz vor unbefugtem Zutritt zu Informationsverarbeitungsanlagen
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung
- **Zugriffskontrolle**: Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Integrität

- **Weitergabekontrolle**: Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
- angemessene **Wiederherstellbarkeit**;

STAND 18.06.2026