



# Allgemeine Geschäftsbedingungen «Planik»

Version 1.6, de, 01.09.2023



Mit Planik steht dem Kunden eine moderne Webapplikation zur Verfügung, die ihm die Erstellung von Personaleinsatzplänen erleichtert (nachfolgend «Planik»). Planik ist ein Produkt der Planik AG (nachfolgend „Planik“) und wird als Software-as-a-Service angeboten. Die vorliegenden AGB regeln die Nutzung von Planik durch den Kunden.

Aus Gründen der Lesbarkeit wurde die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.



1 Vertragsgegenstand.....	3
2 Recht auf Onlinenutzung.....	3
3 Pflichten des Kunden.....	3
4 Verantwortlichkeit des Kunden bez. seiner Inhalte.....	4
5 Leistungserbringung durch Dritte.....	4
6 Vergütung.....	4
7 Betrieb.....	5
8 Gewährleistung und Haftung.....	6
9 Vertraulichkeit und Datenschutz.....	7
10 Kündigung.....	8
11 Vertragsänderung.....	8
12 Schlussbestimmungen.....	8

#### Anhang 1: Vereinbarung über die Auftragsdatenbearbeitung gemäss Art. 9 DSG

1 Gegenstand und Dauer des Auftrags.....	10
2 Ort der Datenbearbeitung.....	10
3 Art der Daten.....	11
4 Kategorien der betroffenen Personen.....	11
5 Pflichten des Auftragnehmers.....	11
6 Technische und organisatorische Massnahmen.....	12
7 Unterauftragsverhältnisse.....	13
8 Kontrollrechte des Auftraggebers.....	13
9 Kopien, Löschung und Rückgabe von Personendaten.....	14

#### Addendum I: Technische und organisatorische Massnahmen

1 Vertraulichkeit.....	15
2 Integrität.....	16
3 Verfügbarkeit und Belastbarkeit.....	16
4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung.....	16
5 Auftragskontrolle: Der Auftragnehmer setzt insbesondere die folgenden Massnahmen um:.....	17



## 1 Vertragsgegenstand

### 1.1 Vertragsinhalt

Planik stellt dem Kunden Planik gegen eine Nutzungsgebühr zur Verfügung. Darin inbegriffen sind auch Wartung und Hosting von Planik, der Support je nach dem vom Kunden gewählten Modul.

### 1.2 Vertragsbestandteile

Ein Vertrag zwischen Planik und dem Kunden besteht in der Regel aus einem Nutzungsvertrag, diesen AGB sowie der Datenschutzerklärung der Planik AG. Die AGB bilden einen integrierenden Bestandteil des Nutzungsvertrages. Im Falle von Widersprüchen zwischen den Vertragsdokumenten gelten die Bestimmungen der Vertragsdokumente in obenstehender Reihenfolge. Eventuell vorhandene, allgemeine Geschäftsbedingungen des Kunden werden wegbedungen.

### 1.3 Vertragsabschluss

Der Vertrag zwischen Planik und dem Kunden kommt durch die Unterzeichnung des Nutzungsvertrags zustande. Der Beginn der Leistungspflichten bzw. des Nutzungsrechts bestimmt sich nach dem Nutzungsvertrag.

## 2 Recht auf Onlinenutzung

Planik erteilt dem Kunden die persönliche, nicht übertragbare und nicht exklusive Nutzungsbefugnis, Planik während der Dauer des Vertrags Online, im Nutzungsvertrag vorgesehenen Umfang, zu nutzen.

Der Kunde ist nicht zur Weiter- und/oder Unterlizenzierung berechtigt. Er darf Planik Dritten nicht zur Verfügung stellen, diese abweichend vom Nutzungsbeschrieb von Planik bearbeiten, ändern oder selbstständig und ohne Einverständnis von Planik vervielfältigen, weiterentwickeln, entschlüsseln oder verwerten. Der Kunde hat kein Recht auf ein Werkexemplar von Planik und damit auch kein Recht auf eine Sicherungskopie.

Die Rechte an den vom Kunden eingepflegten Daten und Inhalten verbleiben beim Kunden. Alle Immaterialgüterrechte an Planik, den dazugehörenden Modulen, Templates, Extensions, Add-ons, Plugins, Dokumentationen usw. und die Rechte an allfälligen kundenspezifischen Weiterentwicklungen verbleiben bei Planik.

## 3 Pflichten des Kunden

### 3.1 Fristgerechte Bezahlung

Der Kunde verpflichtet sich zur fristgerechten Bezahlung der vereinbarten Vergütung.

### 3.2 Nutzung und Zugangsdaten

Der Kunde verpflichtet sich, Planik und die Zugangsdaten ausschliesslich zum vertragsmässigen Zweck und nur während der Dauer des Nutzungsvertrages zu nutzen. Er verpflichtet sich und seine Mitarbeiter zum vertraulichen und sorgfältigen Umgang mit den Zugangsdaten.



### 3.3 Prüfungspflicht und Genehmigungsfolge

Der Kunde hat die Pflicht, für ihn kundenspezifisch ausgeführte Arbeiten bzw. Geliefertes inner 7 Tagen ab Ablieferungs-Notifikation von Planik zu prüfen. Der Kunde ist verpflichtet, allfällige Mängel sofort nach Entdeckung, aber spätestens inner 7 Tagen, schriftlich (auch per Email) der Planik AG mitzuteilen. Ohne solche Mängel-Mitteilung des Kunden inner 7 Tagen, gelten die ausgeführten Arbeiten bzw. das Gelieferte der Planik AG als genehmigt und vom Kunden abgenommen.

### 3.4 Kontaktperson

Der Kunde bezeichnet gegenüber Planik eine entscheidungsfähige Kontaktperson und eine Stellvertretung.

### 3.5 Internetzugang und Browserwahl

Der Kunde ist für seinen Internetzugang für die Benutzung von Planik selber zuständig. Er ist weiter dafür zuständig, für die Benutzung von Planik einen Browser zu verwenden, für den die jeweils aktuelle Version von Planik getestet wurde. Die Liste der getesteten Browser ist unter [www.planik.ch](http://www.planik.ch) einzusehen. Planik steht dem Kunden dafür ein, dass Planik alle Browsersversionen unterstützt, die einen Marktanteil von >10% haben und nicht älter als zwei Jahre sind.

## 4 Verantwortlichkeit des Kunden bez. seiner Inhalte

Der Kunde ist und bleibt Inhaber seiner in Planik gespeicherten Daten. Er ist alleine für die Qualität, Aktualität und Richtigkeit der Inhalte verantwortlich. Er ist auch alleine für die Einhaltung allfälliger arbeitschutz-, und datenschutzrechtlichen sowie regulatorischen Vorgaben gegenüber seinen Mitarbeitern und Dritten verantwortlich.

Für den regelmässigen Export der Pläne und die Archivierung der Inhalte ist der Kunde vollumfänglich selbst verantwortlich.

## 5 Leistungserbringung durch Dritte

Planik hat das Recht, Dritte zur Erbringung von vertraglichen Leistungen beizuziehen.

## 6 Vergütung

### 6.1 Gebühren und deren Anpassung

Die monatliche Nutzungsgebühr für Planik, inklusive definierter Support-, Wartungs- und Hostingleistungen, ist jährlich wiederkehrend jeweils für 12 Monate im Voraus zu bezahlen.

Die vom Kunden zu zahlenden Preise richten sich nach dem im unterzeichneten Nutzungsvertrag aufgeführten Betrag oder nach der jeweiligen Preisliste für die entsprechende Leistung.

Planik kann die im Nutzungsvertrag vereinbarten Gebühren unter Einhaltung einer Mitteilungsfrist von 4 Monaten auf das nächstmögliche Kündigungsdatum gemäss Ziff. 10 dieser AGB anpassen. Sofern der Kunde mit der Erhöhung nicht einverstanden ist, muss er gemäss Ziff. 10 dieser AGB kündigen.



Wurden Planik nicht sämtliche zur Angebotserstellung erforderlichen technischen und organisatorischen Grundlagen zur Kenntnis gebracht oder haben sich diese nach der Angebots-erstellung verändert, bleibt eine Erhöhung der im Nutzungsvertrag genannten Vergütung ausdrücklich vorbehalten.

#### 6.2 Nicht in der Gebühr inbegriffene Leistungen

Sämtliche im Leistungsumfang des unterzeichneten Nutzungsvertrags, resp. des unterzeichneten Angebots, nicht ausdrücklich ausgewiesenen vom Kunden zusätzlich in Anspruch genommenen Leistungen von Planik werden separat in Rechnung gestellt.

Nicht erfasst sind zudem Leistungen, die zur Beseitigung von Störungen, Datenverlusten, etc. erbracht werden, die durch unsachgemäße Bedienung oder Benützung durch den Kunden oder die auf Seiten des Kunden durch unerlaubte Eingriffe Dritter, durch Zufall oder höhere Gewalt erfolgt sind. Entsprechende Leistungen werden dem Kunden separat in Rechnung gestellt.

#### 6.3 Zahlungsmodalitäten

Der Kunde hat die Rechnungen für die erbrachten Leistungen bis zu dem in der Rechnung genannten Fälligkeitsdatum oder innert der angegebenen Zahlungsfrist zu zahlen. Bei fehlender Angabe eines Fälligkeitsdatums oder einer Zahlungsfrist, gilt eine Zahlungsfrist von 30 Tagen ab Datum der Rechnung.

Mit Ablauf der Zahlungsfrist befindet sich der Kunde automatisch, d.h. auch ohne Mahnung, in Verzug. Planik ist berechtigt, für den ausstehenden Betrag einen Verzugszins von 5% pro Jahr zu verlangen. Bei Nichtverfügbarkeit von Planik während 24 Stunden am Stück kann der Kunde die Nutzungsgebühr für die Dauer der Nichtverfügbarkeit zurückfordern. Die Verrechnung weiterer Forderungen durch den Kunden ist ausgeschlossen.

Bei Zahlungsverzug behält sich Planik das Recht vor, den Zugang zu Planik sofort zu unterbrechen und nach Ablauf von drei Mahnläufen den Vertrag fristlos zu beenden. Eine allfällige nicht-Verfügbarkeit von Planik infolge Zahlungsverzugs entbindet den Kunden nicht von der Zahlungspflicht. In jedem Fall erhebt Planik einen Mahnkostenzuschlag von CHF 30.- pro Mahnung.

### 7 Betrieb

#### 7.1 Probleme bei der automatisierten Berechnung von Personaleinsatzplänen mit Planik «Smart»

Der Kunde nimmt zur Kenntnis, dass auf Grund der mathematischen Eigenschaften von Planungsproblemen (NP-Vollständigkeit des Problems) nicht garantiert werden kann, dass die automatisierte Berechnung von Personaleinsatzplänen immer in gleichbleibender Qualität erfolgt. Empfindet der Kunde die Qualität eines Planes als ungenügend, so kann er in Planik die zu verteilenden Dienste manuell den Mitarbeitern zuweisen.

#### 7.2 Wartungsarbeiten

Mit Wartungsarbeiten an Planik oder an den Servern, auf denen Planik läuft, optimiert Planik den Betrieb, die Leistungsfähigkeit und die Qualität von Planik. Der Kunde duldet Nutzungsbeschränkungen, welche durch Wartungsarbeiten entstehen. Planik führt Wartungsar-



beiten vorzugsweise an Randzeiten (zwischen 18.00 Uhr und 8.00 Uhr) durch. Längere Unterbrüche wegen Wartungsarbeiten werden dem Kunden frühzeitig angezeigt.

#### 7.3 Support

Der Support von Planik umfasst die Beantwortung von schriftlich oder telefonisch zugestellten Fragen und Störungsmeldungen durch den Kunden, sowie die damit zusammenhängende Problemanalyse und die einfache Fehlerbehebung durch Planik.

Planik verpflichtet sich, innerhalb von 2 Arbeitstagen nach Eingang einer Anfrage den Kunden zu kontaktieren.

Planik kann vom Kunden verlangen, das Problem vor der Bearbeitung durch Planik in einem vorgegebenen Fehlermeldesystem online zu erfassen.

#### 7.4 Verfügbarkeit

Eine Garantie für eine jederzeitige Verfügbarkeit von Planik und des Supports und für ein Ausbleiben von Funktionsstörungen und Unterbrüche kann nicht übernommen werden. Planik reagiert jedoch schnellstmöglich auf allfällige Ausfälle von Planik. Andere Störungen werden im Rahmen des Supports bearbeitet.

#### 7.5 Neue Versionen, Optionen und Module

Planik kann eine umfassende Aktualisierung oder Weiterentwicklung von Planik oder einzelner Module als neue Version oder Update der Lösung zur Verfügung stellen. Der Kunde ist verpflichtet, die neue Version bzw. das Update einzusetzen.

Planik kann Optionen und Module als kostenpflichtige Erweiterungen anbieten. Für den Kunden besteht keine Verpflichtung diese zu beziehen. Vorbehalten bleibt die Integration einer Option oder eines Moduls als Update oder neue Version der Lösung, ohne dass dadurch zusätzliche Kosten entstehen.

Planik behält sich das Recht vor, im Rahmen des Innovationsprozesses Abläufe und Verhalten von Planik zu modifizieren. Planik garantiert daher nicht, dass sämtliche Funktionen unverändert bleiben. Werden wesentliche Funktionen dahingehend verändert, dass die Funktionalität von Planik für einen Kunden nicht mehr gewährleistet ist, hat dieser das Recht mit sofortiger Wirkung vom Vertrag zurück zu treten.

#### 7.6 Datensicherung

Planik kann einen gesicherten Kundenstand nicht ohne weiteres wiederherstellen. Planik bietet aber kostenpflichtig an, die Dienste gewünschter Pläne auf den Stand einer Datensicherung anzupassen.

### 8 Gewährleistung und Haftung

#### 8.1 Gewährleistung

Planik leistet dem Kunden während der Dauer des Nutzungsvertrages Gewähr dafür, dass Planik bei ordnungsgemässer Nutzung gemäss diesem Nutzungsvertrag über die vereinbarten Spezifikationen verfügt und davon nicht so weit abweicht, dass deren Zweck aufgehoben oder erheblich gemindert ist, sowie dass bei vertragsgemässer Nutzung von Planik durch den Kunden keine Urheberrechte Dritter betreffend Software verletzt werden. Jegliche weitere Gewährleistung wird ausgeschlossen. Die Gewährleistungspflicht von Planik entfällt



insbesondere in dem Umfange, als eine Abweichung von der im Nutzungsvertrag beschriebenen erlaubten Nutzung durch den Kunden erfolgt ist oder auf sonst nicht von Planik zu vertretende Umstände zurückzuführen ist.

Sofern ein Fehler auftritt, für welchen Planik gewährleistungspflichtig ist, hat der Kunde zunächst ausschliesslich Anspruch auf die kostenlose Behebung des Fehlers durch Planik. Der Kunde hat Planik bei der Analyse der Ursachen und Bedingungen des Fehlers sowie bei dessen Behebung in zumutbarem Umfang zu unterstützen.

Gelingt es Planik nicht, den gewährleistungspflichtigen Fehler erfolgreich zu beheben, hat der Kunde - nach freier Wahl von Planik - ausschliesslich Anspruch auf:

- a) Eine Umgehungslösung; oder
- b) Ersatz durch eine andere Software mit gleichwertigem Funktionsumfang; oder
- c) Rücktritt vom Nutzungsvertrag und Rückerstattung der bereits bezahlten Nutzungsgebühren abzüglich dem Zeitanteil für die bereits erfolgte Nutzungsdauer.

Jeglicher Anspruch auf sonstigen Schadenersatz wird ausgeschlossen. Sofern ein Fehler auftritt, für welchen Planik nicht gewährleistungspflichtig ist, ist Planik für den in Behebung eines solchen Mangels aufgewendeten Zeitaufwand zum Stundenansatz gemäss aktueller Preisliste von Planik plus Auslagen und MWST vom Kunden zu entschädigen.

## 8.2 Haftung von Planik

Die in Planik vom Kunden eingegebenen Daten werden über eine hochsichere Verbindung verschlüsselt übertragen. Trotz dem Einsatz hoher Sicherheitsstandards zum Schutz der Daten durch Planik ist die Übertragung von Daten über das Internet nicht vollkommen sicher. Planik kann deshalb keine Garantie für die Sicherheit der Daten vor Hacker-Angriffen, Viren, Trojanern und sonstigen Dritteinwirkungen übernehmen.

## 8.3 Haftung des Kunden und Schadloshaltung

Die Verantwortung für die vom Kunden gemachten Personaleinsatzplanungen, bearbeiteten Personendaten und die Einhaltung der dafür geltenden gesetzlichen und regulatorischen Vorschriften liegt ausschliesslich beim Kunden. Der Kunde verpflichtet sich, Planik gegenüber Ansprüchen seiner Vertragspartner, Arbeitnehmer, Behörden oder Dritten in diesem Zusammenhang vollumfänglich schadlos zu halten, einschließlich für Schäden und Kosten (inklusive Gerichts- und Anwaltskosten), und einen solchen allfälligen Prozess zu übernehmen.

# 9 Vertraulichkeit und Datenschutz

## 9.1 Vertraulichkeit

Die Parteien verpflichten sich selber wie auch ihre Mitarbeiter und beizogene Hilfspersonen zur Wahrung der Vertraulichkeit aller nicht allgemein bekannten Informationen, welche sich auf die geschäftliche Sphäre der anderen Partei beziehen und ihnen bei Vorbereitung und Durchführung dieses Vertrages zugänglich werden. Diese Pflicht bleibt auch nach der Beendigung des Vertragsverhältnisses aufrecht. Planik darf den Kunden bei Einverständnis als Referenz aufführen.

## 9.2 Datenschutz

Im Zusammenhang der Erbringung von Informatikdienstleistungen bearbeitet Planik die Daten des Kunden ausschliesslich zur Erfüllung des Vertrags. Soweit Planik im Sinne des an-



wendbaren Datenschutzrechts als Auftragsdatenbearbeiter Personendaten für den Kunden bearbeitet, tut sie dies ausschliesslich auf die in der Vereinbarung zur Auftragsdatenverarbeitung («**ADV-Vereinbarung**») gemäss Anhang 1 dieser AGB festgelegten Weise und ausschliesslich für die Zwecke des Kunden.

## 10 Kündigung

Der Vertrag wird auf unbestimmte Zeit abgeschlossen. Die Mindestvertragsdauer beträgt 12 Monate. Danach kann jede Partei den Vertrag unter Einhaltung einer Kündigungsfrist von 3 Monaten mit eingeschriebenem Brief auf das Ende eines Kalenderjahres auflösen.

Planik kann den Nutzungsvertrag jederzeit aus wichtigen Gründen mit sofortiger Wirkung auflösen. Dies trifft insbesondere zu, wenn Planik in Verletzung des Nutzungsvertrages verwendet wird oder wenn die vorliegenden AGB trotz schriftlicher Mahnung fortgesetzt missachtet werden. In solchen Fällen bleibt die Zahlungspflicht des Kunden bis zum nächstmöglichen ordentlichen Kündigungsdatum bestehen.

Der Kunde ist selber verantwortlich, nach Beendigung des Vertrags seine Daten aus Planik bei sich zu sichern. Nach Ablauf dieser Frist werden die Daten auf Planik ohne weitere Ankündigung von Planik gelöscht.

## 11 Vertragsänderung

### 11.1 Änderung der AGB

Planik kann diese AGB jederzeit nach eigenem Ermessen anpassen. Vor einer Anpassung wird der Kunde von Planik jeweils notifiziert. Sofern der Kunde mit den Anpassungen nicht einverstanden sein sollte, muss er den Nutzungsvertrag mit Planik gemäss Ziffer 10 dieser AGB innert 30 Tagen per dem nächsten Kündigungstermin kündigen. Sofern der Kunde innerhalb von 30 Tagen nach dieser Notifikation nicht kündet, gelten die geänderten AGB als innerhalb der von Planik kommunizierten Frist als akzeptiert und verbindlich.

### 11.2 Änderungen des Nutzungsvertrages

Änderungen oder Ergänzungen des Nutzungsvertrages bedürfen zu ihrer Rechtswirksamkeit der Unterzeichnung beider Parteien. Dies gilt auch für dieses Schriftformerfordernis.

## 12 Schlussbestimmungen

### 12.1 Übertragung von Rechten auf Dritte

Die Rechte und Pflichten aus dem Vertragsverhältnis dürfen ohne schriftliche Zustimmung von Planik nicht abgetreten oder in sonstiger Weise auf Dritte übertragen werden.

### 12.2 Teilnichtigkeit

Sollten sich einzelne Bestimmungen oder Teile des Vertrages als unwirksam erweisen, so wird dadurch die Gültigkeit der Gesamtvereinbarung im Übrigen nicht berührt. Die Vertragspartner werden in einem solchen Fall den Vertrag so anpassen, dass der mit dem richtigen oder unwirksam gewordenen Teil angestrebte Zweck so weit wie möglich erreicht wird.



### 12.3 Anwendbares Recht und Gerichtsstand

Das vorliegende Vertragsverhältnis untersteht materiellem Schweizerischen Recht, unter Ausschluss des Kollisionsrechts und des Übereinkommens der Vereinigten Nationen über Verträge über den internationalen Warenkauf.

Gerichtsstand für alle entstehenden Rechtsstreitigkeiten ist Bern, Schweiz. Planik ist jedoch berechtigt, ihre Ansprüche nach eigener Wahl auch am Wohnsitz bzw. Sitz des Kunden geltend zu machen.



# Anhang 1: Vereinbarung über die Auftragsdatenbearbeitung gemäss Art. 9 DSG (ADV-Vereinbarung)

Die Planik AG («Auftragnehmer») bietet dem Kunden («Auftraggeber») die Bereitstellung, Wartung und den Betrieb einer webbasierten Software für Personaleinsatzplanung und Arbeitszeiterfassung sowie begleitende Dienstleistungen zu deren Nutzung an. In diesem Zusammenhang bearbeitet der Auftragnehmer personenbezogene Daten, für welche der Auftraggeber verantwortlich ist. Damit ist der Auftragnehmer Auftragsbearbeiter des Auftraggebers.

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz.

## 1 Gegenstand und Dauer des Auftrags

- 1.1 Der Gegenstand dieser Vereinbarung (nachfolgend «Auftrag») ergibt sich aus dem Nutzungsvertrag, auf den hier verwiesen wird (nachfolgend «Hauptvertrag»). Als Hauptvertrag gelten auch sämtliche Bestandteile desselben sowie allfällige Vertragsnachträge und Nachtragsofferten.
- 1.2 Die zu erbringenden Dienstleistungen ergeben sich aus dem Hauptvertrag.
- 1.3 Die Dauer dieses Auftrags entspricht der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen keine darüberhinausgehenden Verpflichtungen ergeben.
- 1.4 Integrierter Bestandteil dieses Auftrags bildet Addendum I – Technische und organisatorische Massnahmen.

## 2 Ort der Datenbearbeitung

- 2.1 Die vertragsgegenständliche Datenbearbeitung wird in der Schweiz, in der EU bzw. in einem EFTA-Staat und in einem Drittstaat, für den ein Angemessenheitsbeschluss des Bundesrats bzw. der Europäischen Kommission vorliegt, erbracht.
- 2.2 Eine Auslagerung der Datenbearbeitung in einen Drittstaat, für den kein Angemessenheitsbeschluss des Bundesrats vorliegt, ist nur unter vorgängiger schriftlicher Zustimmung durch den Auftraggeber möglich. Der Auslagerung in einen solchen Drittstaat gleichgestellt ist die Auslagerung in eine Cloudlösung, falls deren Betreiberin und/oder das die Betreiberin beherrschende Unternehmen dem CLOUD Act der Vereinigten Staaten untersteht.
- 2.3 Der Auftragnehmer stellt sicher, dass er im Rahmen der Auslagerung in einen Drittstaat bzw. eine Cloudlösung gemäss vorstehender Ziffer mittels hinreichender Garantien einen angemessenen Datenschutz gewährleistet und er die besonderen Voraussetzungen gemäss Art. 16 ff. DSG beachtet. Der Auftragnehmer schliesst hierfür bspw. das notwendige Modul der EU-Standardvertragsklauseln («SCCs») vom 4. Juni 2021 ab.
- 2.4 In jedem Fall hat der Auftragnehmer vor der Übermittlung in einen Staat, für den kein Angemessenheitsbeschluss vorliegt, eine Risikoabschätzung in der Form eines Transfer Impact Assessments («TIA») durchzuführen und damit die Gefahr für die Rechte der Betroffenen durch Behördenzugriffe ohne Rechtsweggarantie im entsprechenden Staat zu ermitteln. Eine Übermittlung darf nur erfolgen, wenn das entsprechende Risiko als niedrig im Sinne von Klausel 14 der SCCs eingestuft wurde. Das TIA ist dem Auftraggeber vor der Übermittlung unaufgefordert zur Verfügung zur stellen.



### 3 Art der Daten

Gegenstand der Bearbeitung personenbezogener Daten sind insbesondere folgende Datenarten / -kategorien:

- Personenstammdaten (z. B. Name, Anschrift, Geburtsdatum, Familienstand, Berufsbezeichnung, Firmenzugehörigkeit, Lebensläufe etc.);
- Elektronische Identifikationsdaten (wie IP-Adresse, Elektronische Unterschrift, Verbindungs-/Protokolldaten, Cookies);
- Kommunikationsdaten (z.B. Telefon, E-Mail, PIN, Passwort, Ports, Login);
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
- Vertragsabrechnungsdaten (Arbeitszeiterfassung und variable Lohndaten);

### 4 Kategorien der betroffenen Personen

Die Kategorien der durch die Bearbeitung betroffenen Personen ergeben sich aus der nachfolgenden Aufzählung. Die Kategorien enthalten jeweils ehemalige, aktuelle und potentiell künftige betroffene Personen:

- Beschäftigte;
- Freie Mitarbeiter / Freelancer;

### 5 Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet die Einhaltung folgender Vorgaben:

- 5.1 Personenbezogene Daten dürfen nicht zu anderen als den vom Auftraggeber vorgegebenen Zwecken bearbeitet werden;
- 5.2 Der Auftragnehmer verpflichtet sich zur Wahrung strenger Vertraulichkeit bei der Datenbearbeitung. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Personen ein, die vor Beginn der Datenbearbeitung zur Geheimhaltung verpflichtet und mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort;
- 5.3 Die Bearbeitung erfolgt ausschliesslich gemäss dem Auftrag und der Weisungen des Auftraggebers, es sei denn, dass der Auftragnehmer gesetzlich zu einer abweichenden oder weitergehenden Bearbeitung verpflichtet wird;
- 5.4 Mündliche Weisungen bestätigt der Auftragnehmer sofort und mind. in Textform;
- 5.5 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstösse gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird;
- 5.6 Sofern im anwendbaren Datenschutzrecht vorgeschrieben, führt der Auftragnehmer ein Bearbeitungsverzeichnis, das er dem Auftraggeber auf Anfrage unverzüglich zur Verfügung stellt;
- 5.7 Datenschutzverletzungen meldet der Auftragnehmer unverzüglich an den Auftraggeber. Der Auftragnehmer informiert den Auftraggeber insbesondere im Detail über die Art der Datenschutzverletzung sowie die Kategorie und die Anzahl betroffener Personen und die Anzahl betroffener Datensätze. Der Auftragnehmer trifft die erforderlichen Massnahmen zur Siche-



rung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu ebenfalls unverzüglich mit dem Auftraggeber ab. Zudem teilt der Auftragnehmer unverzüglich mit, wenn es aufgrund der Datenschutzverletzung zu erheblichen Störungen bei der Ausführung des Auftrags kommt oder wenn der Auftragnehmer gegen in diesem Auftrag festgelegten Datenschutzbestimmungen oder -vorgaben verstösst;

- 5.8 Der Auftragnehmer nennt dem Auftraggeber einen Ansprechpartner für im Rahmen dieses Auftrages anfallende Datenschutzfragen und benennt, sofern im anwendbaren Datenschutzrecht vorgeschrieben, einen unternehmensinternen oder -externen Datenschutzverantwortlichen und gibt dem Auftraggeber die entsprechenden Kontaktdaten bekannt;
- 5.9 Der Auftragnehmer unterstützt den Auftraggeber darüber hinaus bei Datenschutz-Folgeabschätzungen und vorherigen Konsultationen;
- 5.10 Der Auftragnehmer informiert den Auftraggeber umgehend über Kontrollhandlungen und Massnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen;
- 5.11 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit den Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben zusammen;
- 5.12 Soweit der Auftraggeber einer Kontrolle der Aufsichtsbehörde, einem Verwaltungs- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsbearbeitung beim Auftragnehmer ausgesetzt ist, wird Letzterer den Auftraggeber nach besten Kräften unterstützen;
- 5.13 Der Auftragnehmer gibt Informationen an Dritte oder Betroffene nur mit vorheriger schriftlicher Zustimmung des Auftraggebers weiter. Direkte Anfragen an den Auftragnehmer gibt dieser unverzüglich an den Auftraggeber weiter;
- 5.14 Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet werden, nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Bearbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer diese Person an den Auftraggeber verweisen und das Ersuchen unverzüglich an den Auftraggeber weiterleiten;
- 5.15 Der Auftragnehmer kontrolliert regelmässig die internen Prozesse sowie die technischen und organisatorischen Massnahmen, um zu gewährleisten, dass die Bearbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt.
- 5.16 Sollten die sich beim Auftragnehmer befindlichen Unterlagen, Daten oder Hardware des Auftraggebers durch Massnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.

## 6 Technische und organisatorische Massnahmen

- 6.1 Der Auftragnehmer hat die Datensicherheit durch geeignete Massnahmen gemäss Art. 8 DSG herzustellen. Die einzelnen Massnahmen ergeben sich aus Anlage I hiernach.
- 6.2 Es handelt sich dabei um Massnahmen der Datensicherheit und zur Gewährleistung eines angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei werden der Stand der Technik, die Kosten und die Art, der Umfang und die Zwecke der Bearbeitung berücksichtigt. Die Massnahmen



gewährleisten insbesondere die zeitnahe Feststellung von Datensicherheits- und Datenschutzverletzungen.

- 6.3 Der Auftragnehmer stellt insbesondere sicher, dass die im Rahmen dieses Auftrages bearbeiteten Daten streng von anderen Datenbanken getrennt sind.
- 6.4 Der Auftragnehmer gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziff. 8 hiernach.
- 6.5 Die technischen und organisatorischen Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden.
- 6.6 Wesentliche Änderungen werden dokumentiert und dem Auftraggeber umgehend schriftlich Textform mitgeteilt. Der Auftragnehmer informiert den Auftraggeber dabei über die von der Anpassung betroffenen Massnahmen nach Addendum I, die Anpassungsgründe, die betroffenen Systeme und die Auswirkung der Anpassung auf den Schutz der vertragsgegenständlichen Personendaten.

## 7 Unterauftragsverhältnisse

- 7.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.
- 7.2 Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Datenbearbeitung beizuziehen

## 8 Kontrollrechte des Auftraggebers

- 8.1 Der Auftraggeber, ggf. dessen Aufsichtsbehörde sowie, falls der Auftraggeber ebenfalls als Auftragsbearbeiter für sie fungiert, dessen Kunden (nachfolgend «Prüfberechtigte») haben das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Das Kontrollrecht des Auftraggebers beschränkt sich auf einmalig alle 12 Monate, insofern der Auftraggeber nicht einen wichtigen Grund benennen kann.
- 8.2 Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig (d.h. innert 10 Arbeitstagen) anzumelden sind, von der Einhaltung dieses Vertrages durch den Auftragnehmer in dessen Geschäftsbetrieb und im von diesem genutzten Rechenzentrum sowie in den Geschäftsräumlichkeiten von allfälligen Unterauftragnehmern zu überzeugen.
- 8.3 Der Auftraggeber und ggf. die weiteren Prüfberechtigten dürfen insbesondere Auskünfte einholen, die Einsichtnahme in gespeicherte Daten und Datenbearbeitungsprogramme verlangen sowie sonstige Kontrollen vor Ort durchführen.
- 8.4 Der Auftragnehmer und ggf. die weiteren Prüfberechtigten sind verpflichtet, die zur Durchführung der Überprüfungen erforderlichen Zugänge und Einsichten zu gewähren, sowie die erforderlichen Abläufe aufzuzeigen, die Auskünfte zu erteilen und die dazu notwendigen Aufzeichnungen zu führen.



- 8.5 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber und ggf. die weiteren Prüfberechtigten jederzeit von der Einhaltung der Pflichten des Auftragnehmers bzw. dessen Unterauftragnehmer aus diesem Auftrag überzeugen können.
- 8.6 Der Auftragnehmer verpflichtet sich, dem Auftraggeber und ggf. die weiteren Prüfberechtigten auf Anforderung jederzeit die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Massnahmen nachzuweisen.
- 8.7 Der Nachweis solcher Massnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.
- 8.8 Der Auftragnehmer ist verpflichtet, sich die Kontrollrechte des Auftraggebers und ggf. den weiteren Prüfberechtigten von seinen Unterauftragnehmern vertraglich einräumen zu lassen.
- 8.9 Ist der Auftragnehmer der Ansicht, dass konkrete Audit- und Kontrollhandlungen den üblichen Umfang übersteigen, hat er dies dem Auftraggeber frühzeitig mitzuteilen, damit eine vorgängige Einigung über die Kosten erfolgen kann. Die Vergütung von allfälligen Unterauftragnehmern ist Sache des Auftragnehmers. Der Vergütungsanspruch entfällt, wenn bei den Kontrollen Verstöße des Auftragnehmers bzw. seiner Unterauftragnehmer gegen die vorliegende Vereinbarung festgestellt werden.
- 9 Kopien, Löschung und Rückgabe von Personendaten
- 9.1 Kopien oder Duplikate der Daten werden nicht ohne Wissen des Auftraggebers erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenbearbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 9.2 Der Auftraggeber entscheidet jederzeit selbst, welche Daten er in der Software löscht. Eine Löschung bedeutet nicht automatisch eine Vernichtung von Daten. Gelöschte Daten sind weiterhin in den Systembackups vorhanden und werden im Rahmen der Backupzyklen nach 2 Jahren überschrieben. Eine definitive Vernichtung kann vom Auftraggeber gegen Aufwandvergütung bestellt werden.
- 9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenbearbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Ende des Auftrags hinaus aufzubewahren. Der Auftragnehmer kann sie zu seiner Entlastung bei Auftragsende dem Auftraggeber übergeben.



# Addendum I – Technische und organisatorische Massnahmen (TOM)

Nachfolgend werden die technischen und organisatorischen Massnahmen beschrieben, die der Auftragnehmer zur Gewährleistung eines angemessenen Sicherheitsniveaus («TOM») ergreift – unter Berücksichtigung der Art, des Umfangs, des Kontextes und des Zwecks der Bearbeitung sowie der Risiken für die Rechte und Freiheiten der betroffenen Personen:

## 1 Vertraulichkeit

### 1.1 Zutrittskontrolle: Der Auftragnehmer gewährleistet, dass kein unbefugter Zutritt zu Datenbearbeitungsanlagen erfolgt.

Die Zutrittskontrolle zum Rechenzentrum und zu den Räumlichkeiten des Auftragnehmers bzw. dessen genehmigte Unterauftragnehmer, in welchen die Daten des Auftraggebers gespeichert bzw. bearbeitet oder Zugangsdaten zu den denselben gespeichert werden, gestaltet sich wie folgt:

- Zutrittskontrollsysteem über Schliessanlage
- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste;
- Überwachungseinrichtung durch Alarmanlage und Aufschaltung auf Sicherheitsdienst;
- Zugangstür ständig geschlossen, Zutritt zu den Unternehmensräumen nur nach Klingeln und Öffnen eines Mitarbeiters;

### 1.2 Zugangskontrolle: Der Auftragnehmer stellt sicher, dass keine unbefugte Systembenutzung erfolgt. Dafür ergreift er folgende Massnahmen:

- Kennwortverfahren (u.a. Komplexitätsanforderungen, Mindestlänge, regelmässiger Wechsel des Kennworts mit Historienverwaltung);
- Zwei oder Multi-Faktor Authentifizierung
- Einrichtung eines Benutzerstammsatzes pro User;
- Passwortschutz der Datenträger;
- Verwendung von zeitgesteuerter Bildschirmsperre mit Passwortschutz;
- bei Bedarf verschlüsseltes WLAN für den internen Gebrauch, zusätzlich entkoppeltes für Gäste in DMZ;
- Ausgefeiltes Firewall-Konzept;

### 1.3 Zugriffskontrolle: Der Auftragnehmer stellt sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von den bearbeiteten personenbezogenen Daten innerhalb des Systems erfolgt. Der Auftragnehmer ergreift die folgenden Massnahmen:

- Festlegung und Kontrolle der Zugriffsbefugnisse differenziert nach Daten, Programmen und Zugriffsarten (Berechtigungskonzept);
- Zeitnahe Einspielen der notwendigen Sicherheitsupdates;
- Ständige Aktualisierung des Virenschutzes;
- Auswertungen über Zugriffe;
- Durchführung externer Sicherheitsaudits;
- Sichere Verwaltung und Verwahrung von Datenträgern/-bestände;



- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network) für eingeschränkten Mitarbeiterkreis;
- 1.4 Trennungskontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitet werden. Der Auftragnehmer ist für die Umsetzung der folgenden Massnahmen besorgt:
- „Mandantenfähigkeit“ der verwendeten Software;
  - Funktionstrennung zwischen Produktion und Test;
- 2 Integrität
- 2.1 Weitergabekontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten bei einer elektronischen Übertragung oder einem Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dafür ergreift er folgende Massnahmen:
- Aufbewahrung in gesichertem Bereich;
- 2.2 Eingabekontrolle: Der Auftragnehmer kontrolliert regelmässig, ob und von wem personenbezogene Daten in Datenbearbeitungssysteme eingegeben, verändert oder entfernt werden sind. Dafür ergreift sie folgende Massnahmen:
- Protokollierungs-Technik durch Festhalten in Datenbank und Protokollauswertung der jeweiligen Benutzer (eindeutige Benutzer-ID);
  - Eindeutige Datenerfassungsanweisung (Handlungsanweisungen);
  - Protokollierung im Ticketsystem.
- 3 Verfügbarkeit und Belastbarkeit
- 3.1 Verfügbarkeitskontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt sind. Der Auftragnehmer ergreift die folgenden Massnahmen:
- Definiertes Backup-Verfahren;
  - Verfügbarkeitsgewährleistung durch redundante Speichersysteme;
  - Unterbrechungsfreie Stromversorgung (gewährleistet beim unterbeauftragtem Rechnungszentrum)
  - Gesicherter und klimatisierter Serverraum (redundant) (gewährleistet beim unterbeauftragtem Rechnungszentrum);
  - Räumlich- und mediumgetrennte Aufbewahrung;
  - Virenschutz / Firewall;
  - Rauchmeldeanlage (gewährleistet beim unterbeauftragtem Rechnungszentrum);
  - CO2-Feuerlöscher (gewährleistet beim unterbeauftragtem Rechnungszentrum);
  - Notfallplan;
- 3.2 Der Auftragnehmer sorgt für eine rasche Wiederherstellbarkeit der Systeme und der Daten des Auftraggebers.
- 4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung
- 4.1 Der Auftragnehmer ist für ein angemessenes Datenschutz-Management und ein Incident-Response-Management besorgt.



- 4.2 Der Auftragnehmer setzt datenschutzfreundliche Voreinstellungen um, damit möglichst wenig personenbezogene Daten bearbeitet werden.
- 5 Auftragskontrolle: Der Auftragnehmer setzt insbesondere die folgenden Massnahmen um:
- Eindeutige Vertragsgestaltung;
  - Formalisierte Auftragserteilung ;
  - Verpflichtung der Mitarbeiter sowie von beauftragten Unternehmen (Dienstleistungsunternehmen, Steuerberater, Wirtschaftsprüfer, Sicherheitsunternehmen und weitere) zum Datenschutz und zur Geheimhaltung;