

Vertrag über die Auftragsdatenverarbeitung

Zwischen
(Name nach HR, Adresse,
PLZ Ort Unternehmen)

und

.....

WORKcontrol Suisse AG

**Bahnhofplatz 1
3011 Bern**

.....

.....

im Folgenden: Auftraggeber

im Folgenden: Auftragnehmer

Adresse Unternehmen

Name nach Handelsregister, Adresse, PLZ, Ort, des Unternehmen
auf Seite 1 (oben) ausfüllen

Unterschriften

Unterschriftsberechtigte Personen auf Seite 12

Rücksendung des Vertrags:

Per Post: WORKcontrol Suisse AG, Bahnhofplatz 1, 3011 Bern

Per Fax: 044 512 88 19

Bitte nicht per E-Mail senden, da nicht rechtsgültig

Vertrag über die Auftragsdatenverarbeitung

INHALT

1 EINLEITUNG, GELTUNGSBEREICH, DEFINITIONEN.....	3
2 GEGENSTAND UND DAUER DER BEARBEITUNG	3
3 ART UND ZWECK DER DATENERHEBUNG, -BEARBEITUNG ODER -NUTZUNG.....	4
4 PFLICHTEN DES AUFTRAGNEHMERS	5
5 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN	6
6 REGELUNGEN ZUR BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN	7
7 UNTERAUFTRAGSVERHÄLTNISSE	7
8 RECHTE UND PFLICHTEN DES AUFTRAGGEBERS (PFLICHTEN DES AUFTRAGGEBERS).....	8
9 MITTEILUNGSPFLICHTEN BEI VERLETZUNG DES SCHUTZES DER AUFTRAGGEBER-DATEN... 	8
10 WEISUNGEN DES AUFTRAGGEBERS.....	9
11 RECHTE DER BETROFFENEN.....	9
12 BEENDIGUNG DES AUFTRAGS.....	10
13 VERGÜTUNG.....	10
14 HAFTUNG	10
15 SONDERKÜNDIGUNGSRECHT	11
16 SONSTIGES.....	11
UNTERSCHRIFT AUFTRAGGEBER	12
ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMS)	13
ANLAGE 2 – ZUGELASSENE SUBUNTERNEHMEN	16
ANLAGE 3 – WEISUNGSBERECHTIGTE PERSONEN	17

1 EINLEITUNG, GELTUNGSBEREICH, DEFINITIONEN

(1) Dieser Vertrag regelt die Rechte und Pflichten von **Auftraggeber** und **Auftragnehmer** (im Folgenden „Parteien“ genannt) im Rahmen einer Bearbeitung von Personendaten (Daten) im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) Daten des Auftraggebers bearbeiten.

(3) Die in diesem Vertrag verwendeten Begriffe sind entsprechend ihrer Definition im Bundesgesetz über den Datenschutz (DSG-CH) zu verstehen. Die **DSG-Begriffe Inhaber der Datensammlung** und **Datenbearbeitung durch Dritte**, sind durch **Verantwortlicher** und **Auftragsverarbeiter** ersetzt. Der Vertrag lehnt sich damit der **Terminologie und Systematik des Europarates sowie der Datenschutzgrundverordnung der Europäischen Union (EU DS-GVO)** an.

2 GEGENSTAND UND DAUER DER BEARBEITUNG

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Bearbeitungen:

Der **Auftragnehmer** stellt eine **elektronische Lösung** (vID-Portal mit Nutzerkonto, vID-Badge, WORKcontrol-App) bereit, die eine effiziente, vereinfachte und kostenoptimierte Umsetzung der gesetzlich geforderten Massnahmen nach dem *Bundesgesetz über die flankierenden Massnahmen bei entsandten Arbeitnehmerinnen und Arbeitnehmern und über die Kontrolle der in Normalarbeitsverträgen vorgesehenen Mindestlöhne* (Entsendegesetz), der *Verordnung des Bundes über die in die Schweiz entsandten Arbeitnehmerinnen und Arbeitnehmer* (Entsendeverordnung) sowie *entsprechenden kantonalen Regelungen* ermöglicht (Hauptvertrag¹ und AGB² zwischen Auftraggeber und Auftragnehmer).

Die Bereitstellung der **elektronischen Lösung** erfordert, dass der Auftragnehmer **Personendaten des Auftraggebers** (dem Subunternehmer im Sinne des Entsendegesetzes) (nachfolgend «Auftraggeber-Daten») bearbeitet, für die der Auftraggeber, im Sinne der datenschutzrechtlichen Vorschriften, als Verantwortlicher gilt.

Zudem übernimmt der Auftragnehmer für den Auftraggeber **Wartung / Support**. Hierbei kann ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten und Rechte der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Angebots.

Der Auftragnehmer erhebt, bearbeitet und nutzt die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers (**Auftragsdatenbearbeitung**).

Der **Auftragnehmer darf die Auftraggeber-Daten ausschliesslich für die Erfüllung des Zwecks (siehe nachfolgend 3.1) verwenden**. Die Auftraggeber-Daten und die Resultate der Auftragsdatenbearbeitung sind vom Auftragnehmer streng vertraulich zu behandeln. Es ist dem Auftragnehmer untersagt Auftraggeber-Daten oder Resultate der Auftragsdatenbearbeitung an Dritte weiterzugeben oder Dritten sonst wie zugänglich zu machen, sofern dies zur Zweckerfüllung nicht zwingend nötig ist (Zutrittskontrolle).

Der Auftraggeber bleibt im datenschutzrechtlichen Sinne verantwortliche Stelle («Herr der Daten»)

2.2 Dauer

Die Bearbeitung erfolgt auf **unbestimmte Zeit** bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

¹ <https://de.workcontrol.ch/tarife>

² <https://de.workcontrol.ch/agb>

3 ART UND ZWECK DER DATENERHEBUNG, -BEARBEITUNG ODER -NUTZUNG

3.1 Art und Zweck der Bearbeitung

Der Auftragnehmer stellt eine **elektronische Lösung** (gemäss Hauptvertrag) bereit, über die der Auftraggeber Daten erfassen, speichern und bearbeiten kann und mit welcher organisatorische Massnahmen zur Umsetzung des Entsendegesetzes (Zutrittskontrolle) in der Praxis ermöglicht werden.

Die Bearbeitung der Personendaten umfasst folgendes:

- **viD-Portal und Nutzerkonto:** Der Auftraggeber erhält nach der Registrierung im viD-Portal vom Auftragnehmer ein **Nutzerkonto**.
- **Registrierungsdossier:** Im Nutzerkonto kann der Auftraggeber die gesetzlich erforderlichen Informationen und Unterlagen seiner Mitarbeiter in einem Registrierungsdossier erfassen.
- **Validierung:** Der Auftragnehmer überprüft die gemäss Entsendegesetz erforderlichen Informationen und Unterlagen des Auftraggebers auf ihre Plausibilität, Erfüllung der gesetzlichen Vorgaben, Vollständigkeit und Aktualität.
- **viD-Badges:** Der Auftraggeber erhält für seine Mitarbeiter vom Auftragnehmer viD-Badges. Diese Badges dienen der Selbstbestätigung über die Einhaltung der minimalen Lohn- und Arbeitsbedingungen sowie als Zugangsinstrument für Baustellen und können mittels der **WORKcontrol-App**, via **viD-Portal am Bildschirm** und via Schnittstellen bei **Zutrittskontrollsystemen von Drittanbietern** zum Zweck der Einhaltung des Entsendegesetzes ausgelesen werden.

Der **Auftraggeber kann den Auftragnehmer anweisen**, in seinem Namen Daten zu bearbeiten (bspw. Datenmigration, -sicherung, -importe, -exporte). Dazu zählt in seiner Funktion als Subunternehmer (im Sinne des Entsendegesetzes) auch das **Bekanntgeben von Personendaten an Erstunternehmer, Lieferanten von Zutrittskontrollsystemen**, sowie **Kontrollbehörden** zum **Zweck der Einhaltung des Entsendegesetzes**.

3.2 Art der Daten

Die elektronische Lösung bietet die Möglichkeit, verschiedene Auftraggeber-Daten zu erfassen und zu bearbeiten.

Der Umfang und die Art der Daten kann auf Wunsch des Auftraggebers erweitert oder eingeschränkt werden. Im Zusammenhang mit der **elektronischen Lösung** werden ausschliesslich Daten von Mitarbeitern bearbeitet, die sich im **Registrierungsdossier** befinden und dazu dienen, den gesetzlichen Vorschriften zu entsprechen. Dazu zählen:

- Personendaten über Nutzer (bspw. Namen, Alter, Geschlecht, Wohnadresse oder Adresse des Arbeitgebers, Notfallnummer)
- Frontal-Vollgesichtsbild der Person für den Badge-Druck
- Arbeitgeber
- Angaben zu GAV-Zugehörigkeit, Lohnklasse und Mindestlohn gemäss GAV
- Kopie eines gültigen Passes / ID / Führerausweis / Ausländerausweis
- Durch Mitarbeiter unterzeichnete Bestätigung des GAV-Mindestlohnes und der Arbeitsbedingungen (nach Vorlage SECO)
- Dokumentation zentrales Mitigrationsinformationssystem (ZEMIS) bei ausländischen Mitarbeitenden (bspw. Niederlassungsausweis, Arbeitsbewilligung)
- Berufliche Qualifikation
- Einsatzvertrag bei temporären Mitarbeitenden

3.3 Kategorien der betroffenen Personen

Von der Bearbeitung betroffen sind:

- Mitarbeiter des Auftraggebers die Zutritt zum Bauperimeter erlangen möchten.

4 PFLICHTEN DES AUFTRAGNEHMERS

In der Regel erfolgt die Erfassung und Bearbeitung der Daten durch den Auftraggeber.

Der Auftraggeber kann den Auftragnehmer anweisen, im Rahmen von Administrations- und Support-Tätigkeiten die Daten des Auftraggebers zu bearbeiten.

(1) Der Auftragnehmer bearbeitet Auftraggeber-Daten **ausschliesslich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen**, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Bearbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Bearbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Bearbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der **Auftragnehmer bestätigt, dass ihm die anwendbaren, allgemeinen datenschutzrechtlichen Vorschriften** bekannt sind. Er beachtet die Grundsätze ordnungsgemässer Datenbearbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Bearbeitung die **Vertraulichkeit streng zu wahren**.

(4) Personen, die Kenntnis von den im Auftrag bearbeiteten Daten erhalten können, haben sich **schriftlich zur Vertraulichkeit zu verpflichten** soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Bearbeitung eingesetzten **Personen** vor Beginn der Bearbeitung mit den **relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden**. **Entsprechende Schulungs- und Sensibilisierungsmassnahmen** sind angemessen regelmässig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernungen laufend angemessen angeleitet und überwacht werden.

(6) Im **Zusammenhang mit der beauftragten Bearbeitung** hat der **Auftragnehmer den Auftraggeber bei Erstellung und Führung des Verzeichnisses der Bearbeitungstätigkeiten sowie bei der Durchführung der Datenschutzfolgeabschätzung zu unterstützen**. Alle erforderlichen Angaben und Dokumentationen sind zu verwalten und dem Auftraggeber auf Anforderung zuzustellen.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der **Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen**, soweit die Bearbeitung im Auftrag betroffen ist.

(8) **Auskünfte an Dritte** oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung **durch den Auftraggeber erteilen**. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Datenschutzbeauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Datenerhebung, -bearbeitung oder -nutzung der Auftraggeber-Daten findet grundsätzlich im Gebiet der Schweiz statt. **Eine Erhebung, Bearbeitung oder Nutzung von Auftraggeber-Daten ausserhalb der Schweiz ist dem Auftragnehmer nur gestattet, wenn die Bedingungen gemäss Art. 6 des Schweizer**

Datenschutzgesetzes (DSG-CH) erfüllt sind und die weiteren Bestimmungen der im Landes des Auftraggebers massgeblichen gesetzlichen Datenschutzregelungen eingehalten sind.

Eine solche **Bearbeitung ausserhalb der Schweiz, der EU oder des EWR, sowie jede Änderung davon bedarf der vorherigen Zustimmung des Auftraggebers**, wobei die Zustimmung nicht unangemessen verweigert werden darf.

Eine Zustimmung kann insbesondere verweigert werden, wenn:

- Die Auftraggeber-Daten oder die Auftragsdatenbearbeitung in ein Drittland übertragen werden sollen bzw. soll, das keinen angemessenen Datenschutz gewährleistet.
- Das Durchsetzen der vorliegenden Vereinbarung durch den Auftraggeber nicht sichergestellt werden kann.

5 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

(1) Die in **Anlage 1 beschriebenen Datensicherheitsmassnahmen werden als verbindlich festgelegt**. Sie definieren das vom **Auftragnehmer geschuldete Minimum**. Die Beschreibung der Massnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmassnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, **solange das hier vereinbarte Niveau nicht unterschritten wird**. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen **Sicherheitsmassnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer** den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die **im Auftrag bearbeiteten Daten von sonstigen Datenbeständen strikt getrennt** werden.

(5) **Kopien oder Duplikate** werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen (Backup), soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Bei der **Bearbeitung von Daten in Privatwohnungen** ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. **Die Bearbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet**.

(7) **Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung**. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(8) Der **Auftragnehmer führt den regelmässigen Nachweis der Erfüllung seiner Pflichten**, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Massnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6 REGELUNGEN ZUR BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN

- (1) Im Rahmen des Auftrags bearbeitete Daten wird der **Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung** oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den **entsprechenden Weisungen des Auftraggebers** wird der **Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages** hinaus Folge leisten.

7 UNTERAUFTRAGSVERHÄLTNISSE

- (1) Die **Beauftragung von Subunternehmern** ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
- (2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich **mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind**. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Passagen der Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die **Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können**. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- (4) Die **Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen**.
- (5) Eine **weitere Subbeauftragung durch den Subunternehmer** ist nur zulässig, wenn für den weiteren Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Die Beauftragung von weiteren Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
- (6) Der **Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Massnahmen sorgfältig** aus.
- (7) Die **Weiterleitung von im Auftrag bearbeiteten Daten an den Subunternehmer** ist erst zulässig, wenn sich der **Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt** hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation auf Anforderung vorzulegen.
- (8) Die Beauftragung von Subunternehmern, die Bearbeitungen im **Auftrag nicht ausschliesslich aus dem Gebiet der Schweiz, der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich**. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
- (9) Der **Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmässig, spätestens alle 12 Monate, angemessen zu überprüfen**. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Anforderung vorzulegen.
- (10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, **so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber**.
- (11) Zurzeit sind die in Anlage 2 mit **Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer** mit der Bearbeitung von Auftraggeber-Daten in dem dort genannten Umfang beschäftigt und durch den

Auftraggeber genehmigt. Die hier festgehaltenen sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(12) **Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen.** Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 RECHTE UND PFLICHTEN DES AUFTRAGGEBERS (PFLICHTEN DES AUFTRAGGEBERS)

(1) Für die **Beurteilung der Zulässigkeit der beauftragten Bearbeitung** sowie für die **Wahrung der Rechte von Betroffenen** ist **allein der Auftraggeber verantwortlich.**

(2) Der **Auftraggeber** erteilt alle **Aufträge, Teilaufträge oder Weisungen schriftlich dokumentiert.** In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der **Auftraggeber informiert** den Auftragnehmer unverzüglich, **wenn er Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse feststellt.**

(4) Der **Auftraggeber** ist **berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer** in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenbearbeitungsprogramme sowie sonstige Kontrollen **vor Ort zu überprüfen.** Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) **Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen.** Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle **12 Monate** statt. **Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich die Kontrolle auf Stichproben beschränken.**

9 MITTEILUNGSPFLICHTEN BEI VERLETZUNG DES SCHUTZES DER AUFTRAGGEBER-DATEN

(1) Der **Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes von Auftraggeber-Daten unverzüglich mit.** Auch **begründete Verdachtsfälle** hierauf **sind mitzuteilen.**

Die Mitteilung hat **spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis** an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- a) eine **Beschreibung der Art der Verletzung des Schutzes der Daten**, soweit möglich mit Angabe der **Kategorien und der ungefähren Zahl der betroffenen Personen**, der betroffenen **Kategorien und der ungefähren Zahl der betroffenen Datensätze**;
- b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- c) eine **Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes der Daten**;
- d) eine **Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung des Schutzes der Daten** und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind **erhebliche Störungen bei der Auftragserledigung** sowie Verstösse des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der **Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Massnahmen von Aufsichtsbehörden oder anderen Dritten**, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den **Auftraggeber bei dessen Pflichten im erforderlichen Umfang zu unterstützen**.

10 WEISUNGEN DES AUFTRAGGEBERS

(1) Der **Auftraggeber** behält sich hinsichtlich der Bearbeitung im Auftrag ein **umfassendes Weisungsrecht** vor.

(2) **Auftraggeber und Auftragnehmer benennen** die zur Erteilung und Annahme von Weisungen ausschliesslich **befugten Personen** in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der **Auftragnehmer wird den Auftraggeber** unverzüglich darauf **aufmerksam machen**, wenn eine vom Auftraggeber erteilte **Weisung** seiner Meinung nach **gegen gesetzliche Vorschriften verstösst**.

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der **Auftragnehmer** hat ihm erteilte **Weisungen und deren Umsetzung zu dokumentieren**.

11 RECHTE DER BETROFFENEN

(1) Die Rechte der durch die Datenbearbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(3) Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von Auftraggeber-daten oder auf Auskunft über die gespeicherten Auftraggeber-Daten, den Zweck der Speicherung und die Empfänger, an die Auftraggeber-Daten regelmässig übermittelt werden (insbesondere gemäss Art. 15 DSG-CH), geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu schützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann.

(4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vorzunehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

12 BEENDIGUNG DES AUFTRAGS

(1) Bei **Beendigung des Auftragsverhältnisses** oder **jederzeit auf Verlangen des Auftraggebers** hat der **Auftragnehmer die im Auftrag bearbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben.**

Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der **Auftragnehmer ist verpflichtet, die Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.**

(3) Der **Auftragnehmer hat den Nachweis der ordnungsgemässen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.**

(4) Dokumentationen, die dem Nachweis der ordnungsgemässen Datenbearbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

13 VERGÜTUNG

Die Vergütung des Auftragnehmers ist abschliessend **im Angebot geregelt.** Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

14 HAFTUNG

(1) Für den Ersatz von Schäden, die eine Person wegen einer **unzulässigen oder unrichtigen Datenbearbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.**

(2) Der **Auftragnehmer trägt die Beweislast dafür, dass ein Schaden** den eine Person wegen einer **unzulässigen oder unrichtigen Datenbearbeitung im Rahmen des Auftragsverhältnisses erleidet nicht Folge eines von ihm zu vertretenden Umstandes ist,** soweit die relevanten Daten von ihm unter dieser Vereinbarung bearbeitet wurden. **Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei,** die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der **Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subunternehmer** im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Abschnitte (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

15 SONDERKÜNDIGUNGSRECHT

(1) Der Auftraggeber kann den **Hauptvertrag** und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („ausserordentliche Kündigung“), **wenn ein schwerwiegender Verstoss des Auftragnehmers gegen die anwendbaren Datenschutzvorschriften** oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmässige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein **schwerwiegender Verstoss** liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Massnahmen in erheblichem Masse nicht erfüllt oder nicht erfüllt hat.

(3) Bei **unerheblichen Verstössen** setzt der Auftraggeber dem Auftragnehmer **eine angemessene Frist zur Abhilfe**. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur ausserordentlichen Kündigung wie in diesem Abschnitt (1) und (2) beschrieben berechtigt.

16 SONSTIGES

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Der Auftraggeber ist Eigentümer der Auftraggeber-Daten sowie sämtlicher Resultate der Auftragsdatenbearbeitung und Inhaber etwaiger Rechte, die die Auftraggeber-Daten oder sämtliche Resultate der Auftragsdatenbearbeitung betreffen.

(3) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Massnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(4) Für Nebenabreden ist die Schriftform erforderlich.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(6) Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages und der AGB. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

UNTERSCHRIFT AUFTRAGGEBER

Ort: Datum:

Unterschriftsberechtigte Person 1:

Name: Vorname:

Unterschrift:

Unterschriftsberechtigte Person 2 (Bei Kollektivunterschrift):

Name: Vorname:

Unterschrift:

Name Subunternehmen nach Handelsregister:

.....

ANLAGE 1 – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOMS)

Anlage 1.1 TOMs des Auftragnehmers

Im Folgenden werden die **technischen und organisatorischen Massnahmen** zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der **Auftragnehmer** einrichtet und laufend aufrechterhält.

Ziel ist die Gewährleistung insbesondere der **Vertraulichkeit, Integrität und Verfügbarkeit** der vom Auftraggeber und nach Anweisung vom Auftragnehmer bearbeiteten Informationen.

Nachfolgende Details beziehen sich zum Teil auf spezifische Eigenheiten im Zusammenhang mit der Datenbearbeitung durch **WORKcontrol Suisse AG**.

1 Vertraulichkeit

a) Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.
Interne Verwaltungssysteme:
<ul style="list-style-type: none"> • Schliessanlage • Badge-System

b) Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.
Interne Verwaltungssysteme:
<ul style="list-style-type: none"> • Passwortgeschützter Zugang zum Portal-Backend • Verschlüsselte Datenübertragung • Arbeitsstationen mit verschlüsselten Laufwerken • Arbeitsstationen teilweise mit Fingerabdruck-Scanner ausgestattet

c) Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen ausserhalb eingeräumter Berechtigungen sind zu verhindern.
Interne Verwaltungssysteme:
<ul style="list-style-type: none"> • Benutzermanagement mit Rechteverwaltung • Aufzeichnung in den Datenbanken wer wann und von wo aus welche Mutationen an Daten vorgenommen hat

d) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu bearbeiten.
Interne Verwaltungssysteme:
<ul style="list-style-type: none"> • Hier nicht anwendbar

e) Pseudonymisierung

Die Bearbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Massnahmen unterliegen.

Interne Verwaltungssysteme:

- Personen- wie auch Unternehmensdaten, zugehörige Dokumente, Daten der Badge-Ausweise und allfällig nachfolgende Berechtigungen (Zutritte zu Bauperimetern) sind mittels 256 Bit-Verschlüsselung in den Datenbanken abgespeichert.

2 Integrität

a) Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) von Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.

Interne Verwaltungssysteme:

- Sämtliche Übermittlungen erfolgen über verschlüsselte Kanäle (mind. 1024 Bit)

b) Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Interne Verwaltungssysteme:

- Eingaben, Änderungen und Löschung der Daten werden protokolliert.
- Differenzierte Benutzerberechtigungen (Lesen, Ändern, Löschen)

3 Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Interne Verwaltungssysteme:

- Laufende, verschlüsselte Backups auf internen wie externen Systemen

b) Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Systeme müssen die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

Interne Verwaltungssysteme:

- Gespiegelte, getrennte Applikations- und Datenbank-Server an verschiedenen Standorten in der Schweiz (keine Server im Ausland), Load-Balancer, USV-Absicherungen, Hard- und Software-Firewall, Antispam und Antivirus auf allen Server-Systemen im Einsatz

4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

a) Kontrollverfahren

Ein Verfahren zur regelmässigen Überprüfung , Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmassnahmen ist zu implementieren.
Interne Verwaltungssysteme:
<ul style="list-style-type: none">• Server werden wöchentlich überprüft und fortlaufend (live) monitored

b) Auftragskontrolle

Es ist sicherzustellen, dass Daten, die im Auftrag durch Dienstleister (Subunternehmen) bearbeitet werden, nur gemäss der Weisung des Auftragnehmers bearbeitet werden.
Interne Verwaltungssysteme:
<ul style="list-style-type: none">• Ist gewährleistet dank klaren Weisungsrechten• Direkte Kommunikation Auftragnehmer - Dienstleister• Archivierungspflicht Kommunikation Auftragnehmer - Dienstleisterr

ANLAGE 2 – ZUGELASSENE SUBUNTERNEHMEN

Die Zusammenarbeit mit folgenden Subunternehmer ist zugelassen:

- vipKIS GmbH, CH-8810 Horgen

Subunternehmer werden unverzüglich benannt, sobald sie zum Einsatz kommen.

ANLAGE 3 – WEISUNGSBERECHTIGE PERSONEN

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Auftraggeber

- Die durch den Auftraggeber als Unternehmens-Administrator festgelegten Benutzer. Die Festlegung erfolgt bei erstmaligem Login im Rahmen der Signup-Acceptance und kann anschliessend durch den Auftraggeber angepasst werden.

Auftragnehmer

- Alle Vertreter der GL der WORKcontrol Suisse AG
- Alle Vertreter des VR der WORKcontrol Suisse AG
- Alle Vertreter der GL der vipKIS GmbH