Für die leichtere Lesbarkeit werden nachfolgend die jeweiligen männlichen Formen sowohl für männliche als auch für weibliche Personen verwendet.

1 VEREINBARUNG ZUM UMGANG MIT PERSONENBEZOGENEN ODER -BEZIEHBAREN DATEN

§ 1 Verpflichtung zur Einhaltung des Datengeheimnisses

(1) Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt.

(2) Der AN verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen durch den AN nur in dem Umfang und in der Art und Weise verarbeitet werden, wie es dem AN zur Erfüllung der ihm übertragenen Aufgaben erforderlich ist.

(3) Des Weiteren ist es dem AN untersagt, die Sicherheit der Verarbeitung von personenbezogenen Daten in einer Weise zu verletzen, die zu einer unbefugten Verarbeitung im Sinne der DSGVO führt.

(4) Personenbezogene Daten des AN können im Rahmen der Zweckbestimmung des Dienstverhältnisses und unter Beachtung der einschlägigen Datenschutzvorschriften gespeichert, übermittelt sowie im Rahmen der gesetzlichen Bestimmungen weitergegeben werden. Diese Zustimmung erstreckt sich auch auf die notwendige Weitergabe und Verarbeitung seiner personenbezogenen Daten innerhalb des Konzernverbundes Zur Information über die Natur der vom Dienstgeber verarbeiteten personenbezogenen Daten, die Zwecke der Datenverarbeitung, die Rechtsgrundlagen für die Datenverarbeitung und damit zusammenhängende Angelegenheiten, gilt die Datenschutzinformation für Mitarbeiter in der jeweils gültigen Fassung.

(5) Der AN verpflichtet sich unbeschadet sonstiger gesetzlicher Verpflichtungen zur umfassenden Einhaltung des Datenschutzes und der Datensicherheit des AG und wird alle Umstände, die mit seinem Arbeitsverhältnis, dem AG, dessen Mitarbeitern oder Kunden sowie Betriebs- und Geschäftsgeheimnissen zusammenhängen, geheim halten. Der AN wird das Datengeheimnis gemäß § 53 BDSG wahren und daher personenbezogene Daten aus Datenverarbeitungen, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht. Es ist ihm untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Der AN darf personenbezogene Daten nur zweckgebunden bzw. im Rahmen seiner Tätigkeit oder Anstellung des AG übermitteln.

(6) Im Falle einer Verletzung oder bei Bekanntwerden werden einer Verletzung des Schutzes personenbezogener Daten („Datenschutzvorfall“) wird der AN unverzüglich eine Meldung an die zuständige interne Meldestelle vornehmen.

§ 2 Tätigkeitsbezogener Umgang mit personenbezogenen Daten

(1) Soweit die Tätigkeit des AN Zugriff auf Telekommunikationsinhalte oder-verkehrsdaten eröffnet, ist ein Zugriff ausschließlich in dem Umfang zulässig, der durch eine ausdrückliche Weisung, eine wirksame Einwilligung der Betroffenen oder eine gesetzliche Befugnis gedeckt ist (§ 3 TDDDG, § 206 StGB).

(2) Werden im Rahmen der Tätigkeiten personenbezogene Daten verarbeitet, die von Sozialleistungsträgern übermittelt wurden und dem Sozialgeheimnis unterliegen (§ 35 SGB I, §§ 67 ff. SGB X), hat der AN diese Informationen mindestens in dem Umfang geheim zu halten, wie es der übermittelnden Stelle obliegt. Jede Nutzung oder Offenlegung ohne Rechtsgrundlage ist untersagt.

§ 3 Rechtsfolgen und Schadensersatzansprüche

(1) Ein Verstoß gegen diese Verpflichtung stellt eine Verletzung von arbeitsvertraglichen Pflichten und ggf. speziellen Geheimhaltungspflichten dar und kann geahndet werden.

(2) Schuldhafte Verstöße gegen diese Verpflichtung können ferner zu zivilrechtlichen Schadensersatzansprüche führen und ggf. nach Art. 83 Abs. 4 DSGVO und §§ 42, 43 BDSG mit Freiheits- oder Geldstrafe geahndet werden.

§ 4 Schlussbestimmungen

(1) Sollte eine Bestimmung dieser Vereinbarung unwirksam, undurchführbar oder nichtig sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien verpflichten sich, die unwirksame, undurchführbare oder nichtige Bestimmung durch eine wirksame und durchführbare Bestimmung zu ersetzen, die dem am Nächsten kommt, was die Parteien in wirksamer Weise zum Zeitpunkt dieser Vereinbarung vereinbart hätten, wenn sie die Unwirksamkeit, Undurchführbarkeit oder Nichtigkeit gekannt hätten. Gleiches gilt für eine Lücke in dieser Vereinbarung.

(2) Diese Vereinbarung unterliegt ausschließlich deutschem Recht und gilt auch nach Beendigung der Tätigkeit weiter.

(3) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Für den Arbeitgeber

Timo Kob
Digital signiert von Timo Kob
DN: cn=Timo Kob, ou=SEC, email=kob@hisolutions.com
Datum: 2025.07.22 14:57:50 +02'00'

Frank Lüdeking
Digital signiert von Frank Lüdeking
DN: cn=Frank Lüdeking, ou=Zentrale, email=Luedeking@hisolutions.com
Grund: i.V.
Datum: 2025.07.18 08:56:10 +02'00'

Prof. Timo Kob	i. V. Frank Lüdeking
Vorstand	Director Business Administration

2 VERTRAULICHKEITS- UND GEHEIMHALTUNGSVEREINBARUNG

Vorbemerkung

Zum Schutze der bei dem AG vorhandenen geschäftlichen, persönlichen und sonstigen Informationen und zum Zwecke der Wahrung der Geschäftsgeheimnisse des AG vereinbaren die Parteien folgendes:

§ 1 Definitionen

(1) Vertrauliche Informationen im Sinne dieser Vereinbarung sind alle wirtschaftlichen, technischen und sonstigen Daten, Mitteilungen, Schriftstücke und ähnliches, einschließlich textlicher, tabellarischer, grafischer, fotografischer, technischer, zeichnerischer, elektronischer, mündlicher oder sonstiger Aufzeichnungen und Mitteilungen, die üblicherweise nicht allgemein bekannt und nicht ohne weiteres zugänglich sind und einen wirtschaftlichen Wert besitzen, durch entsprechende angemessene Sicherheitsmaßnahmen geschützt sind und an deren Geheimhaltung der AG ein berechtigtes Interesse hat. Dies gilt insbesondere für Informationen, die:

a. in irgendeinem Bezug zu den Geschäftspartnern des AG stehen,
b. sonstige personenbezogene Daten enthalten sowie
c. sämtliche, den AG selbst betreffende, nicht öffentlich bekannte Informationen, wie etwa dessen Buchhaltung, eigene Rechtsstreitigkeiten oder Ähnliches (z. B. Geschäftsgeheimnisse, Produkte, Herstellungsprozesse, Know-how, Erfindungen, geschäftliche Beziehungen, Geschäftsstrategien, Businesspläne, Finanzplanung, Personalangelegenheiten, digital verkörperte Informationen).

(2) Keine vertraulichen Informationen im Sinne dieser Vertraulichkeitsvereinbarung sind Informationen, die

a. zur Zeit ihrer Zugänglichmachung durch die jeweilige Partei bereits offenkundig waren,
b. zur Zeit ihrer Zugänglichmachung durch die jeweilige Partei der anderen Partei bereits bekannt waren,
c. der jeweiligen Partei ohne Verstoß gegen die vorliegende Vertraulichkeitsvereinbarung von dritter Seite berechtigterweise bekanntgegeben werden oder aufgrund rechtlicher Vorschriften oder Anordnung eines zuständigen Gerichts, einer Behörde oder sonstigen Einrichtung diesen offenzulegen sind, wobei die andere Partei hierüber – soweit gesetzlich zulässig – unverzüglich vorab zu informieren ist.

Das Vorliegen der vorgenannten Ausnahmen hat die Partei, die sich darauf beruft, zu beweisen.

(3) Dritte im Sinne dieser Vereinbarung sind Wettbewerber oder Parteien, Behörden und sonstige Dritte, die nicht mit dem AG identisch sind. Als Dritte gelten auch Mitarbeitende des AG, die diese Kenntnisse, Informationen oder Daten für ihre Arbeit nicht benötigen.

§ 2 Umfang der Verschwiegenheit und Weitergabe

(1) Dem AN ist bekannt, dass er aufgrund seines Arbeitsverhältnisses mit dem AG Kenntnis von vertraulichen Informationen erlangt hat und/oder erlangen wird. Alle vertraulichen Informationen dürfen nur für dienstliche Zwecke verwendet werden, in deren Zusammenhang sie dem AN bekannt geworden sind, nicht jedoch für Zwecke Dritter oder des AN selbst.

(2) Sowohl während als auch nach Beendigung des Arbeitsverhältnisses- unabhängig von der Art und Weise und den Gründen der Beendigung des Arbeitsverhältnisses- ist es dem AN untersagt, Informationen, die ihm über Angelegenheiten des Unternehmens des AG und der Kunden und/oder Geschäftsbeziehungen des AG bekannt geworden sind, an Dritte weiterzugeben, und zwar im weitesten Sinne des Wortes, von denen der AN wusste oder hätte wissen müssen, dass diese Kenntnisse, Informationen oder Daten geheim sind.

(3) Der AN verpflichtet sich, keine vertraulichen Informationen an Dritte weiterzugeben, es sei denn, der AG stimmt der Weitergabe zuvor schriftlich zu oder ordnet im Rahmen der Geschäftsbeziehung die Weitergabe vertraulicher Informationen ausdrücklich an, soweit eine gesetzliche Verpflichtung zur Mitteilung an Dritte besteht.

(4) Die Weitergabe vertraulicher Informationen an Dritte innerhalb von Projekten ist zulässig, wenn die Weitergabe der Erfüllung des Projektauftrags dient und nicht gegen Geheimhaltungsvereinbarungen verstößt.

(5) Die Weitergabe vertraulicher Informationen im Rahmen von Vertriebsaktivitäten ist zulässig, soweit sie nicht gegen Geheimhaltungsvereinbarungen verstößt, für die Gewinnung des Projektauftrags erforderlich ist und nicht schutzwürdige Interessen des Unternehmens überwiegen.

(6) Eine Weitergabe im vorstehenden Sinne liegt vor, wenn Dritten vertrauliche Informationen zugänglich werden und der AN dies zu vertreten hat. Eine Weitergabe liegt auch vor, wenn vertrauliche Informationen nicht hinreichend vor der Kenntnisnahme durch Dritte geschützt werden. Eine Weitergabe liegt nicht vor, soweit vertrauliche Informationen nach Unterzeichnung dieser Vereinbarung öffentlich oder Dritten bekannt werden, ohne dass der AN dies zu vertreten hat.

(7) Unterlagen und Datenträger, die vertrauliche Informationen enthalten, dürfen nur aus den Geschäftsräumen verbracht oder transportiert werden, sofern ein geschäftliches Erfordernis vorhanden ist. Werden solche Unterlagen und Datenträger nicht mehr benötigt, sind diese bei der IT zur Vernichtung abzugeben.

(8) Ist der AN aufgrund gerichtlicher oder gesetzlicher Bestimmungen verpflichtet, vertrauliche Informationen an Dritte weiterzugeben, wird der AN dem AG diese Verpflichtung unverzüglich anzeigen, sobald er selbst Kenntnis von dieser Verpflichtung erlangt hat.

(9) Eine Offenlegung vertraulicher Informationen gegenüber verbundenen Unternehmen der HiSolutions AG ist nur zulässig, wenn die Offenlegung für die berufliche Tätigkeit erforderlich ist und das verbundene Unternehmen ebenfalls zur Einhaltung der Bestimmungen dieser Vertraulichkeitsvereinbarung verpflichtet wird. Der AN ist verpflichtet, den AG über die Offenlegung der vertraulichen Informationen unverzüglich zu unterrichten.

(10) Firmeneigentum (z. B. Laptop und Diensthandys) sowie sämtliche Korrespondenzen, Notizen, Zeichnungen, Modelle, EDV-Dateien und sonstige Datenträger usw., die sich auf die Angelegenheiten des AG beziehen, sind vom AN auf Verlangen des AG, spätestens jedoch am letzten Tag des Arbeitsverhältnisses, unverzüglich an den AG zurückzugeben.

§ 3 Informationsaustausch mit Geschäftspartnern

(1) Vertrauliche Informationen werden mit einem Geschäftspartner insoweit ausgetauscht, als dies für die Geschäftsbeziehung erforderlich oder nützlich ist.

§ 4 Verschlusssachen

(1) Dem AN ist bekannt, dass Dokumente und Materialien Verschlusssachen (§4 Abs. 1 SÜG) sein können, die in verschiedene Geheimhaltungsgrade unterteilt sind. Solche Dokumente und Materialien sind durch einen entsprechenden Aufdruck auf den Seiten und/oder Titelblatt entsprechend gekennzeichnet. Der AN hat auf solche Kennzeichnungen zu achten.

(2) Sollte der AN im Rahmen seiner Tätigkeit als AN oder bei der Verwendung vom AG zur Verfügung gestellten Arbeitsmittel mit nationalen Verschlusssachen (§4 Abs. 1 SÜG) sowie ausländischen Verschlusssachen und Verschlusssachen zwischenstaatlicher Organisationen (z. B. NATO, EU, OCCAR) unerwartet in Kontakt kommen (z. B. durch unerwartete Zusendung, durch unerwartetes Vorfinden in einem zugriffsberechtigten Ordner), ist der AG unverzüglich darüber zu informieren.

(3) Dem AN sind Arbeiten mit Verschlusssachen (§4 Abs. 1 SÜG) jedes Geheimhaltungsgrades ohne vorherige Belehrung durch ein(e)n Geheimschutzbeauftragte(n) des AG untersagt.

§ 5 Administrative Tätigkeiten

(1) Dem AN sind, sofern er administrative Tätigkeiten an IT-Systemen oder Anwendungen durchführt, folgende Regelungen bekannt:

a. Administrative Berechtigungen sowie die damit verbundenen Informationen sind personengebunden und dürfen nicht weitergegeben werden.
b. Kennwörter für administrative Berechtigungen sind sicher durch Passwortmanager zu verwalten.
c. Alle Zugriffs- und Verwaltungsrechte im Einklang mit den zum Zeitpunkt gültigen Regelungen zu nutzen.
d. Die Vertraulichkeit der Kommunikation gemäß § 3 TDDDG einzuhalten.

§ 6 Rechtsfolgen und Schadensersatzansprüche

(1) Der AN hat mit Schadenersatzansprüchen und disziplinarischen Maßnahmen seitens des AG oder mit strafrechtlichen Konsequenzen gemäß den Vorgaben des Gesetzes zum Schutz von Geschäftsgeheimnissen (§23 GeschGehG), zu rechnen, wenn er sich Zugang zu Geschäfts- oder Betriebsgeheimnisse verschafft, unbefugt erlangt, offenlegt oder anderweitig nutzt. Dies gilt auch für den Missbrauch von administrativen Zugängen, um unberechtigt Informationen zu erlangen.

(2) Die Verletzung von Betriebs- und Geschäftsgeheimnissen ist nach den § 23 GeschGehG strafbar und kann mit Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe geahndet werden. Derjenige, der Geschäfts- und Betriebsgeheimnisse verletzt, ist zum Ersatz des daraus entstandenen Schadens nach § 10 GeschGehG verpflichtet.

(3) Die Gesetzesbestimmungen § 201 ff StGB und §§ 280, 311 II BGB werden vom AN zur Kenntnis genommen.

§ 7 Schlussbestimmungen

(1) Sollte eine Bestimmung dieser Vereinbarung unwirksam, undurchführbar oder nichtig sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien verpflichten sich, die unwirksame, undurchführbare oder nichtige Bestimmung durch eine wirksame und durchführbare Bestimmung zu ersetzen, die dem am Nächsten kommt, was die Parteien in wirksamer Weise zum Zeitpunkt dieser Vereinbarung vereinbart hätten, wenn sie die Unwirksamkeit, Undurchführbarkeit oder Nichtigkeit gekannt hätten. Gleiches gilt für eine Lücke in dieser Vereinbarung.

(2) Diese Vereinbarung unterliegt ausschließlich deutschem Recht und gilt auch nach Beendigung der Tätigkeit weiter.

(3) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Für den Arbeitgeber

Timo Kob
Digital signiert von Timo Kob
DN: cn=Timo Kob, ou=SEC, email=kob@hisolutions.com
Datum: 2025.07.22 14:58:12 +02'00'

Frank Lüdeking
Digital signiert von Frank Lüdeking
DN: cn=Frank Lüdeking, ou=Zentrale, email=Luedeking@hisolutions.com
Grund: i.V.
Datum: 2025.07.18 08:56:36 +02'00'

Prof. Timo Kob	i. V. Frank Lüdeking
Vorstand	Director Business Administration

3 VEREINBARUNG ZUR NUTZUNG VON FOTO- UND VIDEOAUFNAHMEN

Vorbemerkung

Zum Anfertigen von Fotoaufnahmen, Video- und/oder Tonaufzeichnungen während des Beschäftigungsverhältnisses, vereinbaren die Parteien folgendes:

§ 1 Einwilligung (Bitte auf beigefügten Übersichtsblatt ankreuzen)

(4) Der AN ist damit einverstanden, dass der AG, im Rahmen der Durchführung des Beschäftigungsverhältnisses Abbildungen, Fotos, Tonaufnahmen und Videoaufzeichnungen sowie Angaben zur Person (z. B. Vor- und Nachname) und/oder Tätigkeit des AN, gemäß der von ihm angegebenen Verwendungszwecke auf dem Dokument „Vereinbarung zum Anstellungsvertrag“, verwenden darf.

(5) Die Aufnahmen des AN dürfen im Rahmen der vom AN angekreuzten Zwecke genutzt, vervielfältigt, verbreitet und ggf. öffentlich weitergegeben werden.

(6) Der AN bestätigt, dass die Einwilligung freiwillig erfolgt.

(7) Die Verwendung von Fotos und ausgewählten, sachlich angemessenen personenbezogenen Daten im Zusammenhang mit der arbeitsvertraglich vereinbarten Tätigkeit (z. B. im Intranet, Beraterprofil, Funktion im Unternehmen, Erhalt eines Mitarbeiterausweises, in Angeboten und Vergabeverfahren) und dem daraus sich ergebenen berechtigtem Interesse des AG, bedarf es keiner gesonderten Einverständniserklärung.

§ 2 Weitere Verwendung durch Dritte

(1) Dem AN ist bewusst, dass
   a. Foto-, Video- und Tonaufzeichnungen bei der Veröffentlichung im Internet abrufbar sind.
   b. mit geeigneten Suchmaschinen personenbezogene Daten im Internet aufgefunden und die auf Bildnissen dargestellten Personen u. U. auch identifiziert werden können. Dadurch besteht auch die Möglichkeit, durch Zusammenführung dieser Daten und Informationen mit anderen im Internet vorhandenen Daten Persönlichkeitsprofile zu bilden und zusätzliche Nutzungsmöglichkeiten, z. B. für Zwecke der Werbung, zu erschließen und
   c. aufgrund der Möglichkeiten des weltweiten Abrufs und Speicherung der Daten durch andere Stellen oder Personen im Falle eines Widerrufs der Einwilligung und trotz Entfernung der Daten und Bildnisse von den Internetseiten des AG sowie sonstiger Verwendung im WWW eine weitere Nutzung durch andere Stellen oder Personen oder ein Auffinden über Archivfunktionen von Suchmaschinen nicht ausgeschlossen werden kann.

(2) Eine Weiterverwendung von Foto- und Videoaufnahmen durch Dritte kann daher nicht generell ausgeschlossen werden.

§ 3 Widerruf

(1) Die Einwilligung gemäß §1 Absatz 1 kann jederzeit und ohne Angabe von Gründen in Textform (z. B. Brief oder E-Mail), mit Wirkung für die Zukunft widerrufen werden. Dem AN entstehen dadurch keine negativen Folgen.

(2) Die jeweiligen Daten werden bei einem Widerruf unverzüglich, sofern im verhältnismäßigen Rahmen zum Aufwand und Machbarkeit, aus dem onlinebezogenen Angebot entfernt und künftig nicht mehr für neue Druckprodukte verwendet.

(3) Eine Weiterverwendung bereits erstellter Drucksachen oder anderweitige Einwilligungserklärungen bleiben von der Erklärung unberührt.

Für den Arbeitgeber

Timo Kob
Digital signiert von Timo Kob
DN: cn=Timo Kob, ou=SEC, email=kob@hisolutions.com
Datum: 2025.07.22 14:58:25 +02'00'

Frank Lüdeking
Digital signiert von Frank Lüdeking
DN: cn=Frank Lüdeking, ou=Zentrale, email=Luedeking@hisolutions.com
Grund: i.V.
Datum: 2025.07.18 08:56:49 +02'00'

Prof. Timo Kob	i. V. Frank Lüdeking
Vorstand	Director Business Administration

4 WEISUNG FÜR ZUGANG UND UMGANG MIT KOMMUNIKATIONSSYSTEMEN UND -DIENSTEN

Vorbemerkung

Diese Weisung regelt die Grundsätze für den Zugang und die Nutzung der Kommunikationssysteme und-dienste des AG. Ziel dieser Weisung ist die Herstellung der Transparenz der Nutzungsbedingungen und der Maßnahmen zur Protokollierung und Kontrolle zum Schutze von Informationen, die Sicherung der Persönlichkeitsrechte der AN und die Gewährleistung des Schutzes von personenbezogenen Daten.

§ 1 Organisatorische Grundsätze

(1) Die elektronischen Kommunikationssysteme und-dienste stehen dem AN primär als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung.

(2) Die Absicherung des Zugangs zum Internet wird durch diverse Sicherheitsmechanismen (z. B. eine Firewall, Virenschutzprogramme etc.) unter der Verantwortung und Leitung des AG sichergestellt.

(3) Die Installation, Konfiguration und Administration von Kommunikationssystemen und-diensten oder sonstigem (z. B. Web-Browsern) erfolgt durch die IT.

(4) Arbeitsplätze mit einem Internetzugang werden wirksam durch diverse Sicherheitsmechanismen vor Schadsoftware gesichert. Diese Programme dürfen durch Beschäftigte nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für den Einsatz von Filterprogrammen, die den Zugriff auf Angebote mit rechtswidrigen oder strafbaren Inhalten sperren sowie für alle Sicherheitsprogramme und-einstellungen.

§ 2 Zulässigkeit der Nutzung

(1) Die private Nutzung sowie die Nutzung privater Peripherie mit den geschäftlichen Kommunikationssystemen und –dienste ist, unter dem Vorbehalt des Widerrufs, in geringfügigem Umfang zulässig, soweit die Aufgabenerfüllung, die Sicherheit des IT-Systems sowie geltenden Sicherheitsvorgaben nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben oder den Betrieb des Unternehmens hat.

(2) Das Abrufen von für den AG kostenverursachenden Informationen oder Inhalten/Anwendungen aus dem Internet für den Dienstgebrauch ist beim Budgetverantwortlichen zu beantragen. Für das Abrufen von kostenverursachenden Informationen oder Inhalten/Anwendungen für den Privatgebrauch ist der AN selbst verantwortlich. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden, die den Interessen des AG entgegenstehen.

(3) Der AN nimmt zur Kenntnis, dass eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg nicht erfolgt. Die Protokollierung und Kontrolle gemäß §§ 6 und 7 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung von dienstlichen Kommunikationssystemen und-diensten.

(4) Dokumente, die sensible personenbezogene Daten beinhalten, dürfen außerhalb der Netze des AG nicht unverschlüsselt übertragen werden.

(5) Das Abrufen und Ausführen von Programmen aus und im Internet ist nur von durch die IT bekannt gegebenen Anbietern gestattet, soweit deren Inhalte für den dienstlichen Gebrauch benötigt werden. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Ermöglicht die Berechtigung des AN das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, ist das vorher von der IT genehmigen zu lassen. Das Ausführen von aktiven Inhalten (z. B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Anbietern gestattet. Die Einstellungen in den zugehörigen Anwendungen werden von der IT vorgenommen.

(6) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen sind nur mit den von der IT dafür freigegebenen Tools und Zugängen erlaubt. Der Fernzugriff auf Systeme für private Zwecke ist von dienstlichen Systemen aus untersagt.

(7) Die Internet-Telefonie und Bildtelefonie sind grundsätzlich nur mit der dafür freigegebenen Software und Hardware zulässig. Die Teilnahme an Online-Meetings anderer Anbieter darf nur über entsprechende webbasierte Lösungen ohne lokal installierte Komponenten erfolgen.

(8) Mit Beendigung des Beschäftigungsverhältnisses steht die geschäftliche E-Mail-Adresse des AN nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Der AN ist angehalten, seine privaten Kommunikationspartner über diesen Umstand zu informieren. Eingehende E-Mails werden temporär, zur Aufrechterhaltung des Dienstbetriebes, an zuständige Beschäftigte weitergeleitet.

(9) Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Nutzung der Kommunikationssysteme und-dienste beschränkt werden.

§ 3 Verhaltensgrundsätze

(1) Grundsätzlich gelten die Regelungen und weitere Richtlinien des Informationssicherheitsmanagements des AG. Diese Regelungen sind im Intranet veröffentlicht und sind vom AN regelmäßig zur Kenntnis zu nehmen.

(2) Der AN hat jede Nutzung der Kommunikationssysteme und-dienste zu unterlassen, die geeignet ist, den Interessen des AG oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Unternehmensnetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt.

§ 4 Information und Unterrichtung

(1) Der AN wird durch den AG über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet und für den sicheren und wirtschaftlichen Umgang mit diesen Systemen informiert.

(2) Der AG ist durch den AN umgehend zu unterrichten, wenn der AN bei der *privaten* Nutzung der elektronischen Kommunikationssysteme oder-dienste in Kontakt mit Verschlusssachen (nach § 4 Abs.1 SÜG) kommt.

(3) Der AG ist durch den AN umgehend zu unterrichten, wenn der AN bei der *dienstlichen* Nutzung der elektronischen Kommunikationssysteme oder-dienste *unerwartet* in Kontakt mit Verschlusssachen (nach §4 Abs.1 SÜG) kommt.

§ 5 Verantwortlichkeit

(1) Der AN nimmt zur Kenntnis, dass trotz des Einsatzes von Firewalls oder Systemen und Software zum Schutz vor Schadsoftware das Ausspähen und Manipulieren von Daten durch Dritte nicht mit absoluter Sicherheit ausgeschlossen werden kann.

§ 6 Protokollierung und Kontrolle

(1) Aufgrund gesetzlicher Anforderungen, zum Schutz der Mitarbeiterdaten, vertraglicher Verpflichtungen und zur Gefahrenabwehr wird die Kommunikation durch Sicherheitsmechanismen (wie z. B. Firewalls, SIEM, Spam-Filter sowie Virenscanner, mittels eigener Systeme und durch externe Dienstleister) auf Schadsoftware und Unregelmäßigkeiten geprüft und bei Verdachtsfällen weiterverarbeitet.

(2) Zusätzlich führt der AG aus den o. g. Gründen Sicherheitskontrollen/Penetrationstests durch.

(3) Bei der Protokollierung und Prüfung werden div. Informationen aufgezeichnet (z. B. Datum/Uhrzeit, IP-Adressen von Absender und Empfänger, aufgerufene Websites, Login Verhalten).

(4) Die Protokolldateien nach Absatz 3 werden zu Zwecken der
   a. Analyse und Korrektur technischer Fehler
   b. Gewährleistung der Systemsicherheit
   c. Optimierung des Netzes
   d. statistischen Feststellung des Gesamtnutzungsvolumens und
   e. Stichprobenkontrollen und Auswertungen gemäß Absatz 1

   verwendet.

(5) Die Protokolldateien werden durch berechtigte Personen des AG regelmäßig stichprobenhaft gesichtet und in aggregierter Form, ohne Identifizierungsmerkmalen, ausgewertet. Der Datenschutzbeauftragte wird bei der Auswertung beteiligt.

(6) Der Zugriff auf Protokolldateien gem. Abs. 3 ist auf die befähigten Personen beschränkt. Diese hat eine entsprechende Vereinbarung zum Datenschutz unterschrieben. Darüber hinaus ist er hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf strafrechtliche Konsequenzen bei Verstößen hingewiesen worden.

(7) Die Protokolldateien werden, sofern kein Verdacht zur weiteren Kontrolle und Auswertung vorliegt, in Abstimmung mit dem Datenschutz und der Informationssicherheit regelmäßig gelöscht.

(8) Der AN nimmt hiermit zur Kenntnis, dass die Kontrolle und Auswertung von Protokolldateien sich auch auf die private Kommunikation erstrecken können.

§ 7 Maßnahmen bei Verstößen oder Missbrauch

(1) Bei Verdacht auf eine missbräuchliche oder unerlaubte Nutzung der Kommunikationssysteme und -dienste (hervorgerufen z. B. durch Kenntnisnahme nicht zulässiger, im Internet angebotener Inhalte) erfolgt unter Beteiligung des Datenschutzbeauftragten eine Überprüfung des Datenverkehrs durch den nach § 6 Abs. 5 beauftragten Personen. Sind weitere Untersuchungsmaßnahmen (z. B. Offenlegung der IP-Adresse des benutzten Arbeitsplatzes oder weitere Überprüfungen) notwendig, werden die gem. § 6 Abs. 5 beauftragten Personen veranlasst. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem AN ausgehändigt wird. Dieser ist anschließend dazu anzuhören.

(2) Ein Verstoß gegen diese Weisung kann für den AN arbeitsrechtliche Folgen aber auch strafrechtliche Konsequenzen haben.

(3) Der AG behält sich vor, bei Verstößen gegen diese Weisung die private Nutzung der Kommunikationssysteme und-dienste im Einzelfall zu untersagen.

§ 8 Einsatz beim Kunden

(1) Diese Weisung gilt auch, sofern der AN Tätigkeiten direkt bei Kunden des AG ausführt. In diesen Fällen sind für eine zulässige Nutzung der Kommunikationssysteme und-dienste vorrangig die Regelungen des Kunden zu beachten.

5 ANLAGE ZU DER VEREINBARUNG FOTO UND VIDEOAUFNAHMEN

1. Verantwortliche Stelle

HiSolutions AG,
Schloßstraße 1
12163 Berlin, Deutschland

Tel: 030 5332890
E-Mail: info@hisolutions.com
Webseite: www.hisolutions.com

2. Kontaktdaten des Datenschutzbeauftragten

Datenschutz@hisolutions.com

3. Zwecke für die personenbezogenen Daten

Zum Anfertigen von Foto-/Tonaufnahmen und Videoaufzeichnungen während des Beschäftigungsverhältnisses sowie die Zwecke in die der AN eingewilligt hat.

4. Rechtsgrundlage der Verarbeitung

Die Nutzung der Fotoaufnahmen erfolgt auf Basis des Beschäftigungsverhältnisses (Art. 6 Abs. 1 lit. b DSGVO i.V.m. & 26 BDSG) sowie der Einwilligung (Art. 6 Abs. 1 lit a) DSGVO) des AN.

5. Empfänger/Kategorien von Empfängern

Eine Übersicht der Stellen, an denen Foto-/Tonaufnahmen und Videoaufzeichnungen weitergeleitet wurden, kann im Bereich HR und Marketing angefragt werden.

6. Übermittlung in ein Drittland

Eine Übermittlung in ein Drittland kann, je nach Einsatzzweck und Mittel, erfolgen. Eine gesonderte Information wird, falls notwendig, vom Datenschutz bereitgestellt.

7. Dauer der Speicherung

Die Dauer ist mind. die Dauer des Beschäftigungsverhältnisses. Je nach Zweck werden nach Ausscheiden aus dem Unternehmen Foto-/Tonaufnahmen und Videoaufzeichnungen, sofern im verhältnismäßigen Rahmen zum Aufwand und Machbarkeit, entfernt und/oder gelöscht.

8. Rechte der Betroffenen

Als Betroffener hast du laut DSGVO ggf. folgende Rechte:

- Auskunft (Art. 15)
- Berichtigung (Art. 16)
- Löschung (Art. 17)
- Einschränkung der Verarbeitung (Art. 18)
- Widerspruch gegen die Verarbeitung (Art. 21)
- ggf. Widerruf der Einwilligung (Art. 7 Abs. 3)

9. Rechte auf Widerruf einer Einwilligung

Du kannst deine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Deinen Widerruf richtest du bitte an die Personalabteilung.

10. Recht auf Beschwerde bei einer Aufsichtsbehörde

Du kannst dich zu jeder Zeit bei einer zuständigen Aufsichtsbehörde zum Umgang mit deinen personenbezogenen Daten beschweren.

11. Bereitstellung der personenbezogenen Daten vorgeschrieben oder erforderlich

Die Bereitstellung der personenbezogenen Daten ist nicht

- gesetzlich oder vertraglich vorgeschrieben,
- für einen Vertragsabschluss erforderlich oder
- in sonstiger Form verpflichtend.

Eine Nichtbereitstellung hat keinerlei negative Folgen.

6 ANLAGE GESETZESAUSZÜGE

Hier findest Du, in exemplarischer Darstellung, die Überschriften bzw. einzelne Paragraphen relevanter Gesetze. Die Darstellung ist keineswegs vollständig und informiere dich bitte selbst über deren Inhalte. Bei weiteren Fragen oder Informationen zu rechtlichen Fragestellungen erhältst du beim Bereich Personal.

Strafgesetzbuch (StGB)

§ 201 – Verletzung der Vertraulichkeit des Wortes

§ 202 – Verletzung des Briefgeheimnisses

§ 202a – Ausspähen von Daten

§ 202b – Abfangen von Daten

§ 202c – Vorbereiten des Ausspähens und Abfangens von Daten

§ 202d – Datenhehlerei

§ 203 – Verletzung von Privatgeheimnissen

§ 206 – Verletzung des Post- oder Fernmeldegeheimnis

§ 303a – Datenveränderung

§ 303b – Computersabotage

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

§ 3 – Vertraulichkeit der Kommunikation- Fernmeldegeheimnis

Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X)

§ 67a – Erhebung von Sozialdaten

§ 78 – Zweckbindung und Geheimhaltungspflichten eines Dritten, an den Daten übermittelt werden

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

§ 4 – Handlungsverbote

§ 10 – Haftung des Rechtsverletzers

§ 23 – Verletzung von Geschäftsgeheimnissen

Bürgerliches Gesetzbuch (BGB)

§ 280 – Schadensersatz wegen Pflichtverletzung

§ 311 – Rechtsgeschäftliche und rechtsgeschäftsähnliche Schuldverhältnisse

Sicherheitsüberprüfungsgesetz (SÜG)

§ 4 – Allgemeine Grundsätze zum Schutz von Verschlusssachen, Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik

Bundesdatenschutzgesetz (BDSG)

§ 42 – Strafvorschriften

§ 53 – Datengeheimnis

Datenschutz-Grundverordnung (DS-GVO)

Art. 4 – Begriffsbestimmungen

Art. 5 – Grundsätze für die Verarbeitung personenbezogener Daten

Art. 6 – Rechtmäßigkeit der Verarbeitung

Art. 82 – Haftung und Recht auf Schadensersatz