SAFECOR
SICHERHEIT UND AUTOMATION

VERTRAG AUFTRAGSVERARBEITUNG

**Beauftragung zur Verarbeitung von personenbezogenen Daten,
Auftrag zur Verarbeitung von Daten unter Berücksichtigung von Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) und § 62 BDSG.**

VERTRAG AUFTRAGSVERARBEITUNG

zwischen

Unternehmen/Institut: _____

Ansprechpartner: _____

Straße, Hausnummer: _____

PLZ, Ort: _____

- Auftraggeber -

und

SAFECOR GmbH
An der Strusbek 28
22926 Ahrensburg
Deutschland

- Auftragnehmer –

(Auftragsverarbeiter)

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

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

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1. Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

2.2. Zu den Arbeiten und Leistungen gehören auch Systemadministration, Konfiguration von Sicherheitssystemen (Kassensystemen, Mietfachanlagen), Systembetreuung, -pflege und -wartung. Das Anlegen von Benutzern auf Server- oder Applikationsebene, das Konvertieren von Daten, das Anlegen und Erfassen von Benutzer-Identifikationsmerkmalen, wie z.B. Ausweis-, Bank oder Biometriedaten, Einrichtung/ Änderung und/oder Löschung von Benutzerberechtigungen, Eingabe, Änderung oder Löschung von Datenbankfeldern.

2.3. Der Auftrag kann auch die Verarbeitung folgender Arten von personenbezogenen Daten beinhalten: Name und Kontaktdaten von Nutzern der Systeme, Protokoll-, Begehungs- oder Logdaten, sowie Authentifizierungsdaten, wie biometrische Daten, Karten-, Ausweis, oder PIN-Code-Daten und ggf. weitere Daten von Betroffenen, die im jeweiligen System des Auftraggebers gespeichert sind.

2.4. Kreis der von der Datenverarbeitung Betroffenen: Beschäftigte des Auftraggebers, ggf. Kunden des Auftraggebers, ggf. Dritte (Dienstleister des Auftraggebers).

2.5. Die Dauer der Verarbeitung entspricht der im Auftrag vereinbarten Laufzeit.

3. Art und Zweck der Verarbeitung

3.1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

3.2. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen Zwecke im Bereich Sicherheitstechnik, Sicherheitssysteme und IT-Support, die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

4. Art der personenbezogenen Daten und Kategorien von Betroffenen

4.1. Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

4.2. Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

5. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen

5.1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

5.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in elektronisch Form (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

5.3. Die vertraglich vereinbarte Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, soweit nicht etwas Anderes vereinbart ist, z.B. über die Produktbeschreibung der beauftragten Leistung.

6. Rechte des Auftraggebers, Pflichten des Auftragnehmers

6.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

6.2. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung nach Möglichkeit den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

6.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

6.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Gleiches gilt für das Fernmeldegeheimnis nach § 88 TKG und – in Kenntnis der Strafbarkeit – für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StGB. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

6.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

6.6. Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen.

6.7. Machen betroffene Person Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

7. Pflichten des Auftraggebers

7.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

7.2. Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

7.3. Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

8. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

8.1. Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicher zu stellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftragnehmer ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

8.2. Die aktuellen technischen und organisatorischen Maßnahmen sind im Anhang aufgeführt.

8.3. Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

8.4. Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

9. Nachweis und Überprüfung

9.1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen -

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

einschließlich Inspektionen -, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer nach vorheriger Terminabstimmung durchgeführt werden. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen. Der Auftragnehmer stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftraggeber zu, sofern der Auftraggeber dem Auftragnehmer eine Kopie des Audit Berichts zur Verfügung stellt.

9.2. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass der Nachweis der Einhaltung unzureichend oder unzutreffend ist, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung für den Auftraggeber dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen. Diese können zu den üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs, nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden.

9.3. Für Informationen zur Prüfung und Unterstützungshandlungen, sowie Vor-Ort-Kontrollen kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand für den Auftragnehmer durch eine Prüfung oder Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

9.4. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige staatliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gelten die vorstehenden Regeln entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

10. Subunternehmer (weitere Auftragsverarbeiter)

10.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

10.2. Die aktuell eingesetzten weiteren Auftragsverarbeiter sind im Anhang 1 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

10.3. Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

10.4. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund innerhalb einer angemessenen Frist nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen.

10.5. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

10.6. Als weitere Auftragsverarbeiter im Sinne dieser Regelung sind nur solche Subunternehmer zu verstehen, die Dienstleistungen erbringen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören solche Nebenleistungen, die sich auf Telekommunikationsleistungen, Druck-/Post-/Transportdienstleistungen, Wartung und Pflege, Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der personenbezogenen Daten, Netze, Dienste, Datenverarbeitungsanlagen und sonstiger IT-Systeme, beziehen.

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

11. Haftung und Schadensersatz

11.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

11.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

12. Vertragslaufzeit, Sonstiges

12.1. Die Vereinbarung beginnt mit dem Abschluss durch den Kunden. Sie endet mit Ende der letzten Rechnungsstellung für die beauftragte Leistung. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

12.2. SAFECOR kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Ergänzend gelten die AGB des Auftragnehmers, abrufbar unter https://www.safecor.de/agb/. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

12.3. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Hamburg. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.

12.4. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

12.5. Für Nebenabreden ist die Schriftform erforderlich.

12.6. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Name, Vorname (Auftraggeber) in Druckbuchstaben: _____

Unterschrift Datenschutzbeauftragter SAFECOR	Datum, Unterschrift Auftraggeber

AV-Verträge müssen nicht ausschließlich schriftlich vorliegen, sondern können auch in elektronischer Form abgeschlossen werden (Art.28, Abs. 9 DSGVO).

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

ANLAGE

GENEHMIGTE SUBUNTERNEHMER / WEITERE AUFTRAGSVERARBEITER
STAND 20180321

Subunternehmer	Land	Adresse	Leistung
KS safe|Mietfachservice GmbH	Deutschland	Poststraße 3, 06729 Elsteraue	Service, Konfiguration, Parametrisierung, Wartung und Pflege
Contecon Software GmbH	Deutschland	Brückenstraße 2, 67551 Worms	Datenkonvertierung, Kartenverarbeitung, Entwicklung, Wartung und Pflege von Software
ELAN Elektronik GmbH	Deutschland	Johannes-Gutenberg-Str. 4, 22941 Bargteheide	Datenkonvertierung, Kartenverarbeitung, Entwicklung und Fertigung elektronischer Anlagen

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN (TOM) GEMÄß ART. 32 DSGVO

1. Vertraulichkeit

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch folgende Maßnahmen:

- Realisierte Implementierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen über Schlüssel- und Chipkartenregelung sowie biometrische Einlass-Systeme
- Begleitung von Fremdpersonal
- Überwachung der Räume, Alarmanlage
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Keine unbefugte Systembenutzung durch folgende Maßnahmen:

- Passwortrichtlinie, Benutzername und Passwort
- Zuordnung von Benutzerrechten
- Realisierte Implementierung von Benutzerprofilen
- Passwortvergabe mit technisch erzwungener Mindestpasswortlänge und –komplexität
- Physisch gesicherter Zugang zu Daten (Server, Datensafes), Sicherheitsschlösser
- Authentifikation mit biometrischen Verfahren
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

- Realisierte Implementierung eines Berechtigungskonzepts, differenzierte Rechte für Lesen, Verändern oder Löschen von Daten
- Eingrenzen von Schnittstellen zur Verhinderung des Exports
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

Trennungsgebot

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, durch:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Festlegung von Datenbankrechten

2. Integrität

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

- Zwingende E-Mail-Verschlüsselung (TLS enforcement)
- Weitergabe von Daten in verschlüsselter Form (optional bei relevanten Informationen)
- Verwendung von VPN-Tunneln (optional und intern bei relevanten Informationen)
- Interne Kommunikation Ende-zu-Ende verschlüsselt

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch:

- Protokollierung
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- Schutzsteckdosenleisten in Serverräumen
- Erstellen eines Notfallplans
- Brandschutz für Serverräume
- Serverräume nicht unter sanitären Anlagen
- Redundantes Backup-Konzept gegen Krypro-Trojaner

Rasche Wiederherstellbarkeit

- Realisierte Implementierung eines Backup-und Recovery - Konzepts
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen werden z.B. folgende geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

Datenschutz-Management

- Implementierung von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten
- Schulung eigener Mitarbeiter und auf Vertraulichkeit und Datenschutz verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter
- Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt

Vorfallreaktionsplan (Incident-Response-Management)

- Anweisungen wie die Zuständigen auf potenzielle Datensicherheitsverletzungen zu reagieren haben (DoS, DDoS, Firewall, Viren oder Malware und Bedrohungen durch Insider)
- Einstufung im Hinblick auf die datenschutzrechtliche Relevanz (Identifikation eines Vorfalls)
- Schaden begrenzen und betroffene Systeme isolieren (Eindämmung)
- Ursache / Auslöser finden, die betroffene Systeme aus produktiver Umgebung entfernen
- Betroffene Systeme in produktive Umgebung re-integrieren, wenn sichergestellt ist, dass keine weiteren Bedrohungen bestehen (Wiederherstellung)
- Regelmäßige Analyse und Definition kritischer Prozesse. Auswahl angemessener Strategien, zur Reduktion von Ausfallrisiken und Verkürzung von möglichen Ausfallzeiten (Notfallvorsorge)
- Dokumentation eines datenschutzrechtlich relevanten Sicherheitsvorfalls
- Nachvollziehbarkeit: durchgeführte Aktionen, Zeitpunkte, das betroffene IT-System (Dokumentation).
- Beweissicherung: sammeln von Beweisen für eine mögliche Strafverfolgung.
- Transparente Information / Meldung: ausschließlich benannte Verantwortliche informieren über Sicherheitsvorfällen die betroffenen internen und externen Stellen nach festgelegter Reihenfolge und Umfang,
- Ablauf für Notfälle (mit Alarmierung, Meldewegen, Notfall-, Wiederanlauf-, Wiederherstellungs- und Geschäftsfortführung, sowie wichtigen Informationen und klare Aufgabenzuordnung)

Datenschutzfreundliche Voreinstellungen

- Optional bei relevanten Anwendungen: Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten, Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.

- Optional bei relevanten Anwendungen: Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Optional bei relevanten Anwendungen: Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/ oder Durchsetzung von Ansprüchen
- Optional bei relevanten Anwendungen: Für Betroffene: Einrichtung einer operativen Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten.

Auftragskontrolle (bei Auftragsverarbeitung i.S.v. Art. 28 DS-GVO) durch:

- Auswahl von Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung jedes Auftragnehmers und seiner Tätigkeiten
- Schriftliche Weisungen an den Auftragnehmer (durch Auftragsdatenverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags nach vorheriger Weisung
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vertragsstrafen bei Verstößen
- Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
- Wirksam vereinbarte Kontrollrechte gegenüber dem Auftragnehmer

© **SAFECOR GmbH**
An der Strusbek 28
22926 Ahrensburg

Internet: www.safecor.de
Kontakt: info@safecor.de
Support: www.safecor.net

Alle Rechte vorbehalten. Jede Verwertung, Reproduktion, Bearbeitung und Weitergabe an Dritte erfordert einer schriftlichen Zustimmung.