Nach Art. 28 der Datenschutz-Grundverordnung (DS-GVO) (den geltenden Datenschutzgesetzen) sind sowohl Binect als Auftragnehmer als auch der Auftraggeber verpflichtet, einen Vertrag zu Auftragsverarbeitung zu schließen.
Mit diesem Vertrag verpflichtet sich Binect als Auftragnehmer, sämtlichen Anforderungen des Datenschutzes im Zusammenhang mit personenbezogenen Daten umfassend und nachprüfbar nachzukommen.

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

dem Auftraggeber als Verantwortlicher

nachstehend Auftraggeber genannt -

und der

Binect GmbH
Brunnenweg 17
64331 Weiterstadt

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Die Daten des Kunden werden nach elektronischer Einlieferung durch den Kunden auf Verarbeitbarkeit überprüft. Geprüft werden die möglichen Standardformate (PDF, LSF, PostScript, AFP) sowie das digitale Layout (Positionierung des Adressfeldes, Seitenränder). Darauf aufbauend werden die Druckdaten für die Weitergabe an den Druckdienstleister aufbereitet.

Im Rahmen dieses Auftrags können Fehler bei der Verarbeitung auftreten. Bei einem Fehler, der im Zusammenhang mit der Nutzung der Binect-Produkte auftritt, wird dem Auftragsverarbeiter in Abstimmung mit dem Auftraggeber erlaubt, Zugriff auf die personenbezogenen Daten des Kunden zu nehmen. Der Zugriff ist ausschließlich für den Zweck der Fehleranalyse vorgesehen. Neben der Fehlerbeseitigung erfolgt eine Kontrolle der Einlieferungs- und Versandprozesse durch die Binect-Administratoren.

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber versendet vom Arbeitsplatz oder aus einer Anwendung (digitale) Postsendungen an einen Server der Binect GmbH. Der Server im Binect Rechenzentrum sammelt und verarbeitet die Sendungen und leitet zu konfigurierbaren Verarbeitungszeiten die Daten an den Druckdienstleister weiter.

Im Rechenzentrum der Binect GmbH werden die Sendungen im Rahmen eines vollautomatisierten Prozesses auf Produzier- und Versendbarkeit geprüft sowie mit spezifischen Druckinformationen angereichert und an den vereinbarten Druckdienstleister weitergeleitet.

Der Druckdienstleister bereitet die Postsendungen für die weitere Verarbeitung auf und druckt, kuvertiert und frankiert die Postsendungen des Auftraggebers.

Die Zustellung der Postsendungen erfolgt durch die Deutsche Post AG.

Bei der Prüfung als auch bei der Datenaufbereitung erfolgt keinerlei inhaltliche Verarbeitung oder Nutzung der Daten, die Vorprüfung erfolgt ausschließlich zur Sicherstellung der Verarbeitungstätigkeit der Datenformate.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung erfolgt ausschließlich in Deutschland.

(2) Art der Daten

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Sendungsdaten (Druckdaten)

(3) Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden des Auftraggebers, die Briefsendungen erhalten
- ☒ Beschäftigte des Auftraggebers, die Briefsendungen erhalten
- ☒ Lieferanten des Auftraggebers, die Briefsendungen erhalten
- ☒ Ansprechpartner des Auftraggebers

3. Technisch-organisatorische Maßnahmen

Die Einhaltung der Datenschutzanforderungen wird von Binect durch geeignete technisch-organisatorische Maßnahmen (TOM) sichergestellt (s. Anlage 1, TOM der Binect).

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

ink solutions GmbH
Grafenstraße 31a
64283 Darmstadt
Deutschland
datenschutz@binect.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Ausgenommen sind Nebenleistungen, bei denen keinerlei Zugriff auf personenbezogene Daten möglich ist.

Der Auftragnehmer ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie technische und organisatorische Maßnahmen zu ergreifen.

(2) Der Auftraggeber genehmigt die Beauftragung der in Anlage 2 genannten Unterauftragnehmer. Die Beauftragung weiterer Unterauftragnehmer durch den Auftragnehmer oder ein Wechsel von Unterauftragnehmern, die in der Anlage 2 dokumentiert sind, ist dem Auftragnehmer nur mit vorheriger Zustimmung durch den Auftraggeber gestattet, die schriftlich oder in Textform zu erfolgen hat. Soweit der Auftragnehmer eine Neubeauftragung von Unterauftragnehmern vornehmen möchte, informiert er den Auftraggeber schriftlich oder in Textform. Der Auftraggeber ist verpflichtet sich hierzu spätestens binnen 7 Tagen schriftlich oder in Textform zu erklären. Andernfalls gilt die Zustimmung zum Wechsel von Unterauftragnehmern als erteilt.

(3) Der Auftragnehmer verpflichtet sich Unterauftragnehmer mit der gebotenen Sorgfalt auszuwählen und diese durch vertragliche, technische und organisatorische Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften, zu verpflichten.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrags durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 und ISO 9001).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Datengeheimnis / Geschäftsgeheimnis / Fernmeldegeheimnis

(1) Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen nach Art. 28 Abs. 3 Satz 2 lit. b DS-GVO zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die personenbezogenen Daten, zu denen sie Zugang haben ausschließlich auf Weisung verarbeiten, es sei denn, dass sie nach dem Recht der Europäischen Union oder dem Recht der Mitgliedsstaaten der Europäischen Union zur Verarbeitung verpflichtet sind. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen der mit der Bearbeitung und der Erfüllung dieses Vertrages betrauten Person (nachfolgend: Mitarbeiter) bzw. dem vom Auftragnehmer beauftragten Unterauftragnehmer und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(2) Die vom Auftragnehmer eingesetzte Mitarbeiter und gegebenenfalls von ihm beauftragten Unterauftragnehmer sind zur absoluten Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet. Insbesondere erfolgte eine Belehrung und Verpflichtung nach den §§ 2, 4 und 23 GeschGehG. Informationen über den Kunden dürfen nur vom Auftraggeber selbst oder vom Auftragnehmer nach vorheriger schriftlicher Zustimmung des Auftraggebers weitergegeben werden, wenn gesetzliche Bestimmungen dies gebieten oder der Kunde eingewilligt hat oder der Auftraggeber zur Erteilung einer Auskunft befugt ist.

(3) Die Verpflichtung dieser Personen auf die Wahrung der Vertraulichkeit nach Absatz 1 muss vor der erstmaligen Aufnahme ihrer Tätigkeit für den Auftraggeber vorgenommen sein und ist dem Auftraggeber auf Verlangen mittels unterschriebener Verpflichtungserklärung nachzuweisen. Sofern im Hauptvertrag keine abweichende Vereinbarung getroffen wurde, gilt die Verpflichtung zur Gewährleistung der Vertraulichkeit nach Absatz 1 über die Beendigung dieses Vertrages hinaus.

(4) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des befassten Mitarbeiters und gegebenenfalls von ihm beauftragte Unterauftragnehmer regelmäßig in den anwendbaren Datenschutzvorschriften geschult werden.

(5) Wirken Personen des Auftragnehmers und gegebenenfalls von ihm beauftragte Unterauftragnehmer am technischen Vorgang der Erbringung von Telekommunikationsdiensten für den Auftraggeber mit, so erstreckt sich diese Sorgfaltspflicht auch auf das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz oder einer entsprechenden anwendbaren gesetzlichen Bestimmung des betreffenden Rechtsraumes. Die Verpflichtung dieser Personen auf die Wahrung des Fernmeldegeheimnisses muss vor der erstmaligen Aufnahme der Tätigkeit für den Auftraggeber vorgenommen sein und ist dem Auftraggeber auf Verlangen mittels unterschriebenen Erklärungsformulars nachzuweisen.

(6) Auskünfte dürfen der Auftragnehmer und gegebenenfalls der von ihm beauftragte Unterauftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(7) Sofern im Rahmen der Auftragsausführung auch Daten verarbeitet werden, die unter ein Berufsgeheimnis (Privatgeheimnis im Sinne von 203 StGB) fallen, gelten die Absätze 1 bis 6 entsprechend. Darüber hinaus gilt:

- Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten sowie andere für den Auftragnehmer tätigen Personen (z. B. Unterauftragnehmer), die Zugang zu solchen Daten haben, sich dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren. Sie sind über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB zu belehren. Dem Auftraggeber sind die Verpflichtungen und die Belehrungen auf Verlangen in geeigneter Weise nachzuweisen.

- Der Auftraggeber weist den Auftragnehmer darauf hin, dass er sich nach § 203 Abs. 4 Satz 1 StGB strafbar macht, sollte er unbefugt ein fremdes, ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt gewordenes, Geheimnis offenbaren. Der Auftraggeber weist den Auftragnehmer auch darauf hin, dass er sich als mitwirkende Person nach § 203 Abs. 4 Satz 2 Nr. 2 StGB strafbar macht, sollte er sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, sofern der Auftragnehmer als mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage 1 – Technisch-organisatorische Maßnahmen

Siehe Dokument: TOM Technisch Organisatorische Maßnahmen.

Anlage 2 – Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
ad-con Adressen- und Lettershopservice GmbH	Florianweg 48 60388 Frankfurt www.ad-con.de	Druck, Kuvertierung, Freimachung
PAPERSHRED Aktenvernichtung	Rheinhessenstraße 23 55129 Mainz www.papershred.de	Datenträgervernichtung
Paragon Customer Communications GmbH	Mühlenstraße 57 41352 Korschenbroich www.paragon-cc.de	Druck, Kuvertierung, Freimachung
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn	Bereitstellung von dynamischen Applikations-Services & Infrastrukturen, Rechenzentrums-Services
Billwerk+ Germany GmbH	Mainzer Landstraße 51 60329 Frankfurt am Main www.billwerk.plus	Vertragsschluss, Zahlungsabwicklung
Amazon Services EMEA SARL	38 avenue John F. Kennedy L-1855 Luxembourg	Rechenzentrum

Anlage 1

TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Gemäß Art. 32 DSGVO - „Sicherheit der Verarbeitung“

Gültig ab: 17.01.2022

Inhaltsverzeichnis

Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen bilden eine Schnittstelle zwischen Datenschutz und Datensicherheit. Die Regelungen zum Schutz der personen-bezogenen Daten gliedern sich nach den verbindlichen Schutzzielen: Vertraulichkeit, Integrität und Verfügbarkeit. Die Einhaltung der Datenschutzanforderungen wird von Binect durch folgende technisch-organisatorische Maßnahmen (TOM) sichergestellt:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird:

- Anweisungen für Maßnahmen bezüglich der Zutrittskontrolle sind nach einem festgelegten Regelwerk nach ISO 27001 vorhanden.
- Die Gebäudesicherung der *Binect GmbH* ist durch entsprechende bauliche Maßnahmen (Schließanlagen, Brandschutztüren) gegeben.
- Personen mit Zutrittsberechtigung werden dokumentiert festgelegt.
- Die Vergabe und der Entzug von Zugangsberechtigungen sind revisionsfähig.
- Die Datenverarbeitung erfolgt in Sicherheitsbereichen mit beschränkten Zutrittswegen.
- Es gibt gesonderte Zutrittsregelungen für betriebsfremde Personen (Besucherausweise, Besucherbuch).
- Betriebsfremden Personen ist der Zutritt nur in Begleitung autorisierter Personen erlaubt.
- Die sicherheitsrelevanten Räumlichkeiten sind mit Sicherheitsschlössern ausgestattet.
- Die Organisation der Schließanlagen wird über eine EDV-gestützte Zutrittsverwaltung geführt.

1.2 Zugangskontrolle

Maßnahmen, mit denen die unbefugte Systemnutzung von Datenverarbeitungs-systemen verhindert wird:

- DV-Anlagen und Terminals sind abschließbar.
- Zentrale Verwaltung von Benutzerberechtigungen.
- Richtlinie zur Passwortgestaltung und Wechselhäufigkeit.
- Externer Zugang für Mitarbeiter nur über gesicherte und verschlüsselte VPN-Verbindung.
- Einsatz von Anti-Virus-Software.
- Mobile Datenträger (Smartphones, Notebooks) außerhalb des Sicherheitsbereichs werden verschlüsselt.
- Vorgaben zur Clear-Desk-Policy im Unternehmen.

1.3 Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Vergabe, Änderung und Entzug von Zugriffsberechtigungen unterliegen einem geregelten Verfahren gemäß ISO 27001.
- Für die Nutzung von Dateien sowie System-, Anwendungs- und Dienstprogrammen sind Benutzercodes erforderlich.
- Alle Zugriffe werden protokolliert. Die Berechtigungen werden maschinell überprüft.
- Die Nutzung von Terminals und den jeweiligen Identifizierungsmerkmalen ist funktionell und/oder zeitlich begrenzt.
- Bei Inaktivität erfolgt eine automatische Bildschirmsperre.
- Die Dateiorganisation erfolgt nach vorgegebenen Richtlinien durch Produktionssysteme.
- Die freien Abfragemöglichkeiten (SQL-Query) von Datenbanken sind eingegrenzt.
- Es besteht die Möglichkeit eines Teilzugriffs auf Datenbestände und Funktionen.
- Dateien sowie Sicherungssoftware werden routinemäßig verschlüsselt.
- Für den Zugriff auf Prozeduren, Verfahren zur Ablaufsteuerung sowie für Befugnisse zur Katalogisierung von Programmen sind differenzierte Zugriffregelungen festgelegt.
- Produktions- und Testdaten werden physisch oder logisch getrennt.
- Beim Einsatz von Fremdsoftware wird gesondert kontrolliert, soweit diese geeignet sind, Sicherungsmaßnahmen zu umgehen.
- Das Vorgehen für Restart-Verfahren ist schriftlich festgelegt.
- Die Vernichtung von Datenträgern erfolgt gem. DIN 66399 und wird protokolliert.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Bei der Datenerhebung, -verarbeitung und -nutzung erfolgt eine logische und physische Trennung der Daten.
- Für Personen, die Daten erheben, verarbeiten und nutzen, sind Benutzerprofile festgelegt.
- Produktions- und Testdaten werden physisch oder logisch getrennt.

1.5 Pseudonymisierung

Die Verarbeitung 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 entsprechend technischen und organisatorischen Maßnahmen unterliegen:

- Druckdaten werden durch Verschlüsselungsverfahren abgesichert.
- Die Erfassung von Informationen zur Abrechnung und für statistische Auswertungen erfolgt auf Basis einer abstrakten Kundennummer.
- Eine Pseudo- und Anonymisierung von Daten erfolgt im Testmanagement.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Es soll verhindert werden, dass Daten unbeabsichtigt geändert oder zerstört werden. Gewährleistung der Echtheit, Vollständigkeit und Zurechenbarkeit.

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Übermittlungswege und Datenempfänger sind festgelegt und werden dokumentiert.
- Die Datenübermittlung und die jeweiligen Datenempfänger werden protokolliert.
- Die Möglichkeit der Auswertung der Übermittlungsprotokolle nach Empfängern und Abrufen ist gegeben.
- Die elektronische Übertragung erfolgt über verschlüsselte Verbindungen.
- Für die Datenleitungen besteht ein Fernwartungskonzept.
- Die Datenübertragung erfolgt unter Hinzuziehung von zusätzlichen Sicherheits- und Verschlüsselungsmaßnahmen (Einsatz kryptographischer Verfahren).
- Fester Bestandteil der Transportkontrolle sind Prüfungen auf Plausibilität, Vollständigkeit und Richtigkeit.

Eine physische Übermittlung von Daten (Datenträger, Briefe etc.) findet im Rahmen der Auftragsverarbeitung nicht statt.

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Datenverarbeitung: Die Übertragung von Daten auf die Server durch Anwender ist durch automatische Identifikation und/oder durch Benutzerzertifikate nachvollziehbar. Es wird protokolliert, wer, wann, wie viele Datenströme an den Server überträgt.
- Zugriffe des Wartungspersonals auf den Server per https werden ebenfalls mit Userangaben protokolliert. Änderungen an Konfigurationsdateien, Aufspielen von Patches und Fixes oder ein Up- oder Download von Daten werden protokolliert.
- Terminals und Terminalnutzer müssen sich gegenüber dem DV-System identifizieren.
- Es erfolgt eine Vergabe und Sicherung von Identifizierungsschlüsseln.
- Terminals und Identifizierungsmerkmale sind auf bestimmte Funktionen begrenzt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind:

- Um die Verfügbarkeit zu sichern, werden für alle schutzwürdigen Objekte Notfallpläne erstellt und im Notfallhandbuch den Mitarbeitern zur Verfügung gestellt.
- Alle Daten werden regelmäßig gesichert. Die Datensicherung erfolgt täglich im externen Rechenzentrum der *Binect GmbH*.
- Die Sicherheitsapplikationen werden über ein Datenbank-Logging zusätzlich kontrolliert.
- Die Daten werden durch erhöhte Verfügbarkeitssysteme und Redundanz gesichert.
- Es wird eine regelmäßige Risiko- und Schwachstellenanalyse nach definierten Schutzzielen durchgeführt.
- Sicherungskopien werden an besonders geschützten Orten innerhalb der Rechenzentren aufbewahrt.
- Recovery-Verfahren gewährleisten die Wiederherstellung von Daten.
- Alle Mitarbeiter werden regelmäßig geschult.
- Fachabteilung und DV-Abteilung sind funktionell getrennt.

3.2 Belastbarkeit, Robustheit und Resilienz

Wesentlicher Faktor für die Belastbarkeit der zur Verfügung gestellten Leistungen ist der Umgang mit der Überschreitung von Kapazitätsgrenzen.

- Durch proaktives Monitoring, Planung außergewöhnlicher Sendungsereignisse in Abstimmung mit den eingebundenen Dienstleistern, Flexibilisierung der Datenverarbeitung und Produktion auf mehrere Systeme und Leistungspartner, wird die Basis geschaffen auch im Überlastfall die geregelte Produktion sicherstellen zu können.
- Als Richtlinie für den Aufbau der Prozesse wurde definiert, dass Verlässlichkeit und Vollständigkeit der Produktion Vorrang gegenüber der Einhaltung von Produktionsterminen hat. Dabei ist eine möglichst umfassende, zeitnahe und automatisierte Transparenz des Prozessablauf zum Kunden zu gewährleisten.

3.3 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit).

- Zur Bewältigung von unvorhersehbaren Krisensituationen stehen Notfall-Anweisungen und -Prozesse gemäß ISO 9001/27001 zur Verfügung.
- IT-Verfahren, Software und IT-Konfiguration werden dokumentiert.
- Alle Daten werden regelmäßig gesichert. Die Wiederherstellbarkeit wird geprüft.
- Softwarestände und Konfiguration unterliegen einer Versionskontrolle.
- Buildprozesse und Deployment werden auf Basis von Containertechnologie automatisiert.
- Sicherungskopien werden an besonders geschützten Orten im *Binect*-Rechenzentrum vorgehalten.
- Ein Schwerpunkt des Informations-Sicherheits-Managementsystems (ISMS) bildet die Risikoanalyse zum Schutz personenbezogener Daten. Die Dokumentation erfolgt mittels Richtlinien und Handbücher.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Die Binect GmbH hat ein Datenschutz-Management-System eingeführt, welches die organisatorischen Maßnahmen, die für die Gewährleistung eines rechtskonformen Umgangs mit personenbezogenen Daten nach Art. 5 und Art. 24 der DSGVO nachvollziehbar darstellt. Im Wesentlichen umfasst dies folgende Prozesse:

- interne Prüfungen vor Beginn neuer Verarbeitungen personenbezogener Daten,
- schriftliche Richtlinien zur Gewährleistung der Grundsätze zur Datenqualität,
- Unterrichtung, Sicherheit und Betroffenenrechte,
- ständige Aktualisierung von Verarbeitungsverzeichnissen,
- Bestellung eines Datenschutzbeauftragten,
- Durchführung von Mitarbeiterschulungen,
- Beschwerde- und Data-Breach-Management

Das Datenschutz-Management System beinhaltet die kontinuierliche Bestandsaufnahme existierender Datenschutzprozesse sowie deren Steuerung und Schulung der Mitarbeiter.

4.2 Incident-Response-Management

Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

- Analog zum Notfall-Management wurden Verantwortlichkeiten, Aufgaben und Meldewege bei Störungen und Sicherheitsvorfällen definiert und allen beteiligten Mitarbeitern kommuniziert.
- Alle relevanten Anwendungen werden auf neu bekannt gewordene Sicherheitsprobleme regelmäßig geprüft. Sofern ein Sicherheitsproblem identifiziert wurde, sind die vorgeschlagenen Maßnahmen zu prüfen und ggf. zu ergreifen.
- Die Nachbereitung von Sicherheitsvorfällen wird dokumentiert.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Personenbezogenen Daten werden nur für den vorbestimmten Verarbeitungszweck vorgehalten. Die Speicherfrist und Zugänglichkeit von Daten entspricht den gesetzlichen Vorgaben (Privacy by Default). Dem Prinzip der Datenminimierung wird entsprochen, indem nur solche Daten erhoben werden, die für das jeweilige Verfahren erforderlich sind. Neben der Datensparsamkeit kommen auch Verschlüsselungstechniken zum Einsatz (Privacy by Design). Ferner existieren Richtlinien zur Nutzerauthentifizierung sowie die technische Umsetzung des Widerspruchsrechts (Art. 21 DSGVO).

4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle).

- Die Auswahl von Auftragnehmern erfolgt unter größter Sorgfalt. Insbesondere in Bezug auf Datenschutz und Datensicherheit.
- Auftragnehmer der Binect GmbH werden regelmäßig auditiert.
- Kompetenzen und Pflichten in Bezug auf Datensicherungsmaßnahmen, Transportregelungen, Aufbewahrungs- und Löschungsvorschriften, Vertragsverletzungen und Versicherungen sind zwischen Auftraggeber und Auftragnehmer festgelegt.
- Die Auftragsverarbeitung erfolgt formalisiert, die Arbeitsergebnisse unterliegen einer strengen Kontrolle.
- Die Sicherheitseinrichtungen beim Auftragnehmer werden kontrolliert.
- Der Auftraggeber hat Zutrittsrecht beim Auftragnehmer.
- Die Einhaltung der technisch-organisatorischen Maßnahmen werden jährlich kontrolliert.