Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

……..

Name und Anschrift

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

PIN AG, Alt- Moabit 91, 10559 Berlin

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftraggeber wird über das PIN eBrief- Portal elektronisch Datensätze für die Erstellung von Briefen an die Auftragnehmerin aufliefern.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsdurchführung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die vom Auftraggeber aufgelieferten Daten werden vom Auftragnehmer drucktechnisch aufbereitet und dann zum Druckdienstleister gesendet, dann vom Druckdienstleister ausgedruckt, kuvertiert und durch den Auftragnehmer physisch zugestellt.

Zweck ist die physische Zustellung der elektronisch aufgelieferten Sendung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten

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

- ☐ Personenstammdaten (Adressdaten, Zugangsdaten)

- ☐ Kommunikationsdaten (E-Mail)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Inhalte der aufgelieferten Daten (Dokumente)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kundendaten des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich, seine innerbetriebliche Organisation entsprechend dem Auftrag so auszugestalten, dass sie den jeweils geltenden Datenschutzanforderungen gerecht werden.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [**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 Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt und dessen Kontaktdaten dem Auftraggeber zum Zweck der

direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 einschließlich der spezialgesetzlichen Vorgaben des Postrechts 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 Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [**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. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
BC Directgroup GmbH	Rigistr. 9, 12277 Berlin	Druckdienstleister
Möller Druck & Verlag GmbH	Zeppelinstraßee 9, 16356 Ahrensfelde	Druckdienstleister
ODS – Office Data Service GmbH	Ehrenbergstraße 16A, 10245 Berlin	Druckdienstleister

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, beim Auftragnehmer jederzeit und ungehindert 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 dieser Vereinbarung 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 DSGVO 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

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer keinen Vergütungsanspruch geltend machen. Die vom Auftragnehmer unter dieser Vereinbarung geschuldeten Pflichten, Handlungen, Beistellungen und Mitwirkungen sind mit der im jeweiligen Auftrag vereinbarten Vergütung für die vom Auftragnehmer geschuldeten Leistungen abgegolten.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

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. 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 28 Tage nach Beendigung der Leistungsdurchführung – hat der Auftragnehmer sämtliche vom Auftraggeber zur Verfügung gestellten Daten, datenschutzgerecht zu vernichten.

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

11. Haftung

(1) Macht eine betroffene Person gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter erfolgreich einen Schaden aufgrund eines Verstoßes gegen die Regelungen der DSGVO gelten, findet Art. 82 DSGVO Anwendung.

(2) Für alle sonstigen Schäden, die die Verantwortlichen durch die Nichteinhaltung einer erteilten Weisung entstehen, haftet der Auftragsverarbeiter entsprechend der gesetzlichen Regelungen.

12. Vertragsänderungen, Salvatorische Klausel

(1) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen zur Ihrer Wirksamkeit der Schrift oder Textform. Das gilt auch für diese Klausel selbst.

(2) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder ihre Rechtswirksamkeit später verlieren, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen Bestimmung gelten die gesetzlichen Vorschriften.

(3) Auf diese Vereinbarung findet das Recht der Bundesrepublik Deutschland unter Ausschluss der Regelungen des Kollisionsrechts Anwendung.

Ort, Datum	Ort, Datum
Auftraggeber (rechtsverbindliche Unterschrift)	Auftragnehmer (rechtsverbindliche Unterschrift)

Anlage 1

Technisch- organisatorische Maßnahmen nach Art. 32 DSGVO

PIN AG

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.0 Zutrittskontrolle Folgende Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanalgen haben:

- [x] Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte, Dongle, PIN, 2- Faktor)
- [x] Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- [x] Sicherheitstüren/ -fenster
- [x] Gitter vor Fenstern/ Türen
- [ ] Zaunanlagen
- [x] Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe
- [ ] Werkschutz/ Pförtner
- [x] Alarmanlage
- [x] Videoüberwachung - Bereich: Sortierung
- [x] Spezielle Schutzvorkehrungen des Serverraums
- [x] Spezielle Schutzvorkehrungen für die Aufbewahrung von Backups/ sonstige Datenträgern
- [x] Nicht reversible Vernichtung von Datenträgern
- [x] Mitarbeiter- und Berechtigungsausweise
- [x] Sperrbereiche
- [x] Besucherregelungen (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch
- [ ] Sonstiges:

1.1 Zugangskontrolle Folgende Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsanalgen haben:

- [x] Persönlicher und individueller User- Log- In bei Anmeldung am System bzw. Unternehmensnetzwerk
- [x] Autorisierungsprozess für Zugangsberechtigungen
- [x] Begrenzung der befugten Benutzer
- [ ] Single- Sign- On
- [x] BIOS- Passwörter
- [x] Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
  10 Zeichen, komplex
- [x] Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- [x] Personalisierte Chipkarten, Token, PIN-/ TAN, etc.
- [ ] Protokollierung des Zugangs
- [x] Zusätzlicher System- Log- In für bestimmte Anwendungen

- [x] Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- [x] Firewall
- [ ] Sonstiges:

1.2 Zugriffskontrolle Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- [x] Verwaltung und Dokumentation von differenzierten Berechtigungen
- [x] Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von EDV-Anlagen
- [ ] Auswertungen/ Protokollierungen von Datenverarbeitungen
- [x] Autorisierungsprozess für Berechtigungen
- [ ] Genehmigungsroutinen
- [ ] Profile/ Rollen
- [x] Verschlüsselung von CD/DVD-, externen Festplatten und/oder Notebooks (z.B. per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- [ ] Maßnahmen zur Verhinderung unbefugten Kopierens von Daten auf externe Datenträger (Kopierschutz, DLP-System)
- [x] Mobile- Device- Managementsystem
- [x] Vier- Augen- Prinzip
- [ ] Funktionstrennung
- [x] Fachkundige Akten- und Datenträgervernichtung nach DIN 66399
- [x] Nicht- reversible Löschung von Datenträgern
- [ ] Sichtschutzfolien für mobile EDV- Systeme
- [ ] Sonstiges:

1.3 Trennungskontrolle Folgende Maßnahmen stellen sicher, dass die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten getrennt verarbeitet werden:

- [ ] Speicherung der Datensätze in physikalisch getrennten Datenbanken
- [ ] Verarbeitung auf getrennten Systemen
- [x] Zugriffsberechtigungen nach funktioneller Zuständigkeit
- [x] Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- [ ] Mandantenfähigkeit von IT- systemen
- [ ] Verwendung von Testaten
- [x] Trennung von Entwicklungs- und Produktionsumgebung
- [ ] Sonstiges:

1.4 Pseudonomysierung Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können:

- [x] Verfahren: Es findet keine Pseudonymisierung der Daten statt, da im Rahmen der Briefdienstleistungserbringung diese Daten im Klartext benötigt werden, um eine ordnungsgemäße Zustellung zu gewährleisten. Werden diese Daten nicht mehr benötigt. erfolgt eine automatisierte Löschung.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO

2.0 Weitergabekontrolle Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Es wurden dafür folgende Maßnahmen implementiert:

- [ ] Verschlüsselung von Email bzw. Email- Anhängen (z.B. WinZip)
- [x] Verschlüsselung des Speichermediums von Notebooks
- [x] Gesicherter File Transfer (z.B.sftp)
- [x] Gesicherter Datentransport (z.B. SSL, ftps, TLS)
- [ ] Verschlüsselung von CD/DVD, externen Festplatten oder USB- Sticks (z.B. True Crypt, Safe Guard Easy, PGP)
- [ ] Physikalsische Transportsicherung
- [ ] Verpackungs- und Versandvorschriften
- [ ] Elektronische Signatur
- [ ] Gesichertes WLAN
- [x] Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Rückrufautomatik, Einmal-Passwort)
- [x] Mobile- Device- Management
- [ ] Data Loss Prevention (DLP)- System
- [x] Regelung zum Umgang mit mobilen Speichermedien (z.B. Notebook, USB- Stick, Mobiltelefon)
- [ ] Protokollierung von Datenübertragung oder Datentransport
- [ ] Protokollierung von lesenden Zugriffen
- [ ] Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- [x] Getunnelte Datenverbindungen (VPN)
- [ ] Sonstiges:

2.1 Eingabekontrolle Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- [x] Zugriffsrechte
- [x] Systemseitige Protokollierung
- [x] Dokumenten- Management- System (DMS) mit Änderungshistorie
- [ ] Sicherheits-/ Protokollierungssoftware
- [x] Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- [ ] Mehraugenprinzip
- [ ] Data Loss Prevention (DLP)
- [ ] Sonstiges:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.0 Verfügbarkeits- und Belastbarkeitskontrolle Durch folgende Maßnahmen wird sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- [ ] Sicherheitskonzept für Software- und IT- Anwendungen
- [x] Backup- Verfahren
- [x] Aufbewahrungsprozess für Backups (brandgeschützter Safe, Banksafe, getrennter Brandabschnitt, etc.)
- [x] Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- [x] Bedarfsgerechtes Einspielen von Sicherheits- Updates
- [x] Spiegeln von Festplatten (Raid-System)
- [x] Unterbrechungsfreie Stromversorgung (USV)
- [x] Geeignete Archivierungsräumlichkeiten für Papierdokumente
- [x] Brandschutz im Serverraum
- [ ] Brandschutz in den Archivierungsräumen
- [x] Klimatisierter Serverraum
- [x] Virenschutz
- [x] Firewall
- [x] Notfallplan
- [ ] Erfolgreiche Notfallübungen
- [x] Redundante, örtlich getrennte Datanaufbewahrung (offsite Storage)
- [ ] Sonstiges:

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

4.0 Datenschutz- Management Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- [ ] Datenschutzleitbild
- [x] Datenschutz- Richtlinien
- [x] Richtlinien/ Anweisungen zur Gewährleistung von technisch- organisatorischen Maßnahmen zur Datensicherheit
- [x] Bestellung eines Datenschutzbeauftragten (Kontaktdaten)

  Olaf Thom, Alt- Moabit 91, 10559 Berlin, Telefon: 030577978184, E-Mail: olaf.thom@pin-ag.de
- [x] Verpflichtung der Mitarbeiter auf das Datengeheimnis
- [x] Hinreichende Schulungen der Mitarbeiter zum Datenschutz/ zur Datensicherheit
- [x] Führung der Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- [x] Durchführung von Datenschutz- Folgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- [ ] Ext. Prüfung/ Auditierung der Informationssicherheit (z.B. nach ISO 27001)
- [ ] Sonstiges:

4.1 Incident- Response- Management Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- [x] Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- [x] Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- [ ] Sonstiges:

4.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsanlagen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminnimierung die Zulässigkeit bestimmter Eingaben bzw. Eingabemöglichkeiten (z.B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung oder die Verfügbarkeit von bestimmten Verarbeitungfunktionen, Protokollierung etc. festgelegt.

- [x] Beispiele: Es werden bei Onlineformularen und eigenen Softwareentwicklungen nur erforderliche Felder als Pflichtfelder deklariert. Entsprechende Zugriffsrechte sichern darüber hinaus den Zugriff nur für befugte Mitarbeiter.

4.3 Auftragskontrolle Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können:

- [x] Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den rechten und Pflichten des Auftragnehmers und Auftraggebers
- [ ] Prozess zur Erteilung und/oder Befolgung von Weisungen
- [x] Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- [x] Kontrolle/ Überprüfung weisungsgebundener Auftragsdurchführung
- [ ] Schulungen/ Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- [x] Unabhängige Auditierung der Weisungsgebundenheit
- [x] Verpflichtung der Mitarbeiter auf das Datengeheimnis
- [ ] Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- [x] formalisiertes Auftragsmanagement
- [ ] dokumentiertes Verfahren zur Auswahl des Dienstleisters
- [x] standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister
- [ ] Sonstiges:

5.0 Kontaktdaten der/des Datenschutzbeauftragten:

Name: Olaf Thom

Telefon: 030 57 79 78 - 184

E-Mail: olaf.thom@pin-ag.de