d.vinci

Einzelvereinbarung
über die Auftragsverarbeitung personenbezogener Daten

Zwischen

dem Kunden

- Auftraggeber -

und

d.vinci HR-Systems GmbH

Nagelsweg 37-39

20097 Hamburg

Deutschland

- Auftragnehmer -

1. Gegenstand der Beauftragung

1) Die Parteien haben einen Rahmenvertrag über die Auftragsverarbeitung personenbezogenen Daten geschlossen, der nunmehr durch diese Einzelvereinbarung ergänzt wird.

2) Anlass des Abschlusses dieser Einzelvereinbarung ist die Beauftragung für die Nutzung des d.vinci Onboarding in dessen Rahmen der Auftragnehmer personenbezogenen Daten im Auftrag für den Auftraggeber verarbeitet.

2. Gegenstand und Zweck der Verarbeitung

1) Gegenstand der Verarbeitung personenbezogenen Daten ist die Erbringung der im Hauptvertrag vereinbarten Leistungen durch den Auftragnehmer für den Auftraggeber.

2) Der Zweck der entsprechenden Verarbeitung der personenbezogenen Daten ergibt sich aus dem Hauptvertrag. Ausschließlich zur Erfüllung dieses Zwecks und im Zusammenhang der insoweit vom Auftragnehmer zu erbringenden Leistungen werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht. Der Zweck umfasst insbesondere die folgenden Aufgaben:

   a) Erfolgreiche Eingliederung von neuen Mitarbeitern in das Unternehmen
   b) Erfolgreiche Eingliederung nach einem Stellenwechsel innerhalb des Unternehmens
   c) Erfolgreiche Wiedereingliederung von Mitarbeitern nach längerer Abwesenheit
   d) Betrieb des d.vinci Onboardings in einem vom Auftragnehmer beauftragten Rechenzentrum
   e) Wartung und Pflege der Software entsprechend den vertraglichen Vereinbarungen

3. Von der Verarbeitung betroffene Arten personenbezogener Daten

Von der Auftragsverarbeitung sind folgende Arten personenbezogenen Daten betroffen:

   a) Adressdaten
   b) Lebensläufe
   c) Zeugnisse (z.B. Arbeitszeugnisse)
   d) Profile von angehenden Mitarbeitern, neuen Mitarbeitern und aktuellen Mitarbeitern
      Unter angehenden Mitarbeitern verstehen wir Bewerber in Vertragsverhandlungen und Bewerber nach erfolgreicher Unterschrift unter den Arbeitsvertrag, jedoch vor dem ersten Arbeitstag.
   e) sonstige Mitarbeiterdaten und -unterlagen, wie z.B. Lichtbilder

   Ob die vom Auftragnehmer zu erbringenden Leistungen und die insoweit getroffenen Vereinbarungen geeignet sind für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, bedarf einer Risikobewertung durch den Auftraggeber.

4. Kategorien der von der Verarbeitung betroffener Personen

Von der Auftragsverarbeitung sind folgende Kategorien von Personen betroffen:

   a) Angehende Mitarbeiter im Unternehmen
   b) Mitarbeiter im Unternehmen
   c) Mitarbeiter als Benutzer der Anwendung d.vinci Onboarding

5. Technische und organisatorische Maßnahmen

Der Auftragnehmer ergreift die im Auftrag verarbeiteten personenbezogenen Daten die in der Anlage 1 und 2 aufgeführten technischen und organisatorischen Maßnahmen.

6. Weisungsberechtigte Personen

1) Die folgenden Personen sind für den Auftraggeber weisungsberechtigt; er kann die Liste der weisungsberechtigten Personen jederzeit durch einseitige Erklärung modifizieren.

   a) alle laut Handelsregister zur rechtsgeschäftlichen Vertretung des Auftraggebers Berechtigten in vertretungsberechtigter Anzahl
   b) alle namentlich benannten Key User des Auftraggebers

2) Der Auftragnehmer erklärt, dass die folgenden Personen für ihn entsprechend empfangsbevollmächtigt sind:

   a) alle laut Handelsregister zur rechtsgeschäftlichen Vertretung des Auftragnehmers Berechtigten in vertretungsberechtigter Anzahl
   b) alle Mitarbeiter der Firma d.vinci, die im Bereich Customer Service tätig sind

7. Unterauftragsverarbeiter

1) Der Auftragnehmer setzt für die Verarbeitung folgenden Unterauftragsverarbeiter ein:

   - pop-interactive GmbH, Wendenstraße 408, 20537 Hamburg

2) Anforderungen an den Subunternehmer pop-interactive GmbH: Die pop-interactive GmbH ist für die eigene regelkonforme Nutzung des Datacenters und alle weiteren benötigten Services wie Netzaufbau, Carrier-Anbindungen, interne Verkabelung und Rackaufbau verantwortlich. Das Datacenter wird zusammen mit der Mr. net Group GmbH & Co in der Wendenstraße in Hamburg betrieben. Infrastrukturelle Vertragsangelegenheiten für den Betrieb des Datacenters erledigt die Mr. net Group GmbH & Co mit den jeweiligen Versorgern und Dienstleistungsunternehmen. Dies beinhaltet auch eine jährliche VdS-Prüfung.

8. Ort der Auftragsverarbeitung

Die Auftragsverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Offenlegung an Drittländer erfolgt nicht.

9. Rückgabe

1) Daten, Datenträger sowie sämtliche sonstige Materialien mit personenbezogenen Daten, die diesem Vertrag unterfallen, sind nach Auftragsende je nach Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Sofern der Auftraggeber eine Weisung zur Löschung erteilt, die vom bisher Vereinbarten abweicht, und hieraus zusätzliche Kosten für den Auftragnehmer entstehen, so trägt diese der Auftraggeber. Die Löschung ist in geeigneter Weise zu dokumentieren. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen erfolgen.

2) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird. Dies gilt nicht, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung des Auftraggebers zur Speicherung der personenbezogenen Daten weiter besteht. In diesem Fall gilt für die Dauer dieser Verpflichtung dieser Vertrag entsprechend weiter.

10. Dauer der Vereinbarung

Die Dauer dieser Einzelvereinbarung richtet sich nach der Laufzeit des Hauptvertrages. Sie kann isoliert nur aus wichtigem Grund gekündigt werden.

d.vinci HR-SYSTEMS
d.vinci HR-Systems GmbH
Nagelsweg 37–39 · 20097 Hamburg

_____	_____
Kunde	d.vinci HR-Systems GmbH

Anlagen

Anlage 1: Technische und organisatorische Maßnahmen – Büroräume

Anlage 2: Technische und organisatorische Maßnahmen – Rechenzentrum

Anlage 1: Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

Die in diesem Dokument beschriebenen Maßnahmen beziehen sich auf den **Standort Nagelsweg 37-39 in Hamburg, an dem die Büroräume im 4. und 5. Stockwerk liegen.** Wie im Betriebskonzept beschrieben werden hier im Regelfall keine Bewerberdaten oder Mitarbeiterdaten verarbeitet. In Ausnahmefällen findet eine Bearbeitung von Bewerberdaten oder Mitarbeiterdaten statt; hierfür gibt es dann stets einen Antrag vom Kunden.

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

a) Zutrittskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- ☑ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☑ Alarmanlage
- ☑ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☑ Nicht-reversible Vernichtung von Datenträgern
- ☑ Mitarbeiter- und Berechtigungsausweise
- ☑ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

b) Zugangskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- ☑ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☑ Autorisierungsprozess für Zugangsberechtigungen
- ☑ Begrenzung der befugten Benutzer
- ☑ BIOS-Passwörter
- ☑ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☑ Protokollierung des Zugangs (ADS- und Firewall-Logs)
- ☑ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☑ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☑ Firewall

c) Zugriffskontrolle || Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- ☑ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☑ Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
- ☑ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☑ Autorisierungsprozess für Berechtigungen
- ☑ Genehmigungsroutinen
- ☑ Profile/Rollen
- ☑ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- ☑ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)
- ☑ Funktionstrennung „Segregation of Duties“
- ☑ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399 (Dienstleister ist zertifiziert)
- ☑ Nicht-reversible Löschung von Datenträgern

d) Trennungskontrolle || Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- ☑ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ☑ Verarbeitung auf getrennten Systemen
- ☑ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☑ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☑ Mandantenfähigkeit von IT-Systemen
- ☑ Verwendung von Testdaten
- ☑ Trennung von Entwicklungs- und Produktionsumgebung

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) || Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

An diesem Standort werden keine Bewerberdaten oder Mitarbeiterdaten verarbeitet.

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

a) 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. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☑ Verschlüsselung des Speichermediums von Laptops
- ☑ Gesicherter File Transfer (z.B. sftp)
- ☑ Gesicherter Datentransport (z.B. SSL, ftps, TLS)
- ☑ Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)
- ☑ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☑ Protokollierung von Datentransport (Backup)
- ☑ Protokollierung von lesenden Zugriffen innerhalb der Anwendung
- ☑ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

b) Eingabekontrolle || Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- ☑ Zugriffsrechte
- ☑ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☑ Mehraugenprinzip

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

Verfügbarkeitskontrolle und Belastbarkeitskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- ☑ Sicherheitskonzept für Software- und IT-Anwendungen
- ☑ Back-Up Verfahren
- ☑ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☑ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☑ Spiegeln von Festplatten
- ☑ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☑ Klimatisierter Serverraum
- ☑ Virenschutz
- ☑ Firewall
- ☑ Notfallplan
- ☑ Erfolgreiche Notfallübungen
- ☑ Redundante, örtlich getrennte Datenaufbewahrung (Off-site Storage)

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

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

- ☑ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ☑ Bestellung eines Datenschutzbeauftragten
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- ☑ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- ☑ Ext. Prüfung/Auditierung der Informationssicherheit (ISO-Zertifizierung 27001)

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

- ☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO)
- ☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Betroffenen (Art. 34 DS-GVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) ||

Die Default-Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

An diesem Standort werden keine Bewerberdaten oder Mitarbeiterdaten verarbeitet.

d) Auftragskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- ☑ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☑ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☑ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☑ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☑ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ formalisiertes Auftragsmanagement
- ☑ dokumentiertes Verfahren zur Auswahl des Dienstleisters

Anlage 2: Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

Die in diesem Dokument beschriebenen Maßnahmen beziehen sich **auf den Standort Wendenstraße 408 in Hamburg, an dem das Rechenzentrum im 3. Stockwerk betrieben wird.** Die Maßnahmen beziehen sich daher auf den Dienstleister, der die Infrastruktur zur Verfügung stellt, sowie die im Rechenzentrum betriebenen Rechner, auf die der Dienstleister keinen Zugriff hat.

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

a) Zutrittskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- ☑ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☑ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ☑ Gitter vor Fenstern/Türen
- ☑ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☑ Alarmanlage
- ☑ Videoüberwachung
- ☑ Spezielle Schutzvorkehrungen des Serverraums: Früherkennung von Bränden und Wassereinbruch
- ☑ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☑ Nicht-reversible Vernichtung von Datenträgern
- ☑ Mitarbeiter- und Berechtigungsausweise
- ☑ Sperrbereiche
- ☑ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

b) Zugangskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- ☑ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☑ Autorisierungsprozess für Zugangsberechtigungen
- ☑ Begrenzung der befugten Benutzer
- ☑ BIOS-Passwörter
- ☑ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☑ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- ☑ Protokollierung des Zugangs

- ☑ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☑ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☑ Firewall

c) Zugriffskontrolle || Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- ☑ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☑ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☑ Autorisierungsprozess für Berechtigungen
- ☑ Genehmigungsroutinen
- ☑ Profile/Rollen
- ☑ Funktionstrennung „Segregation of Duties“, siehe Betriebskonzept.
- ☑ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399

d) Trennungskontrolle || Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- ☑ Speicherung der Datensätze in logisch getrennten Datenbanken (Prinzip: Ein Dienst pro Server, eine Datenbank pro Kunde)
- ☑ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☑ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☑ Mandantenfähigkeit von IT-Systemen
- ☑ Verwendung von Testdaten
- ☑ Trennung von Entwicklungs- und Produktionsumgebung

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) || Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Bei Anlegen des Datensatzes eines Bewerbers oder eines Mitarbeiters wird eine Kennung erzeugt, die im weiteren Verlauf der Verarbeitung verwendet wird.

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

a) 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. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☑ Verschlüsselung des Speichermediums von Laptops
- ☑ Gesicherter Datentransport (z.B. SSL, ftps, TLS)
- ☑ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☑ Protokollierung von Datentransport (Backup)
- ☑ Protokollierung von lesenden Zugriffen innerhalb der Anwendung

b) Eingabekontrolle || Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- ☑ Zugriffsrechte
- ☑ Systemseitige Protokollierungen
- ☑ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

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

Verfügbarkeitskontrolle und Belastbarkeitskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- ☑ Sicherheitskonzept für Software- und IT-Anwendungen
- ☑ Back-Up Verfahren
- ☑ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☑ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☑ Spiegeln von Festplatten
- ☑ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☑ Brand- und/oder Löschwasserschutz des Serverraums
- ☑ Klimatisierter Serverraum
- ☑ Virenschutz
- ☑ Firewall
- ☑ Notfallplan
- ☑ Erfolgreiche Notfallübungen
- ☑ Redundante, örtlich getrennte Datenaufbewahrung (Off-site Storage)

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

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

- ☑ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ☑ Bestellung eines Datenschutzbeauftragten
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- ☑ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- ☑ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- ☑ Ext. Prüfung/Auditierung der Informationssicherheit (ISO-Zertifizierung 27001)

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

- ☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO)
- ☑ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Betroffenen (Art. 34 DS-GVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) || Die Default-Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

- ☑ Es werden nur die für das Onboarding notwendigen Daten eines Bewerbers oder Mitarbeiters erhoben.
- ☑ Beim Export der Daten an Unterauftragnehmer werden nur jene Daten übertragen, die für die Dienstleistung notwendig sind.

d) Auftragskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- ☑ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☑ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☑ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☑ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☑ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ formalisiertes Auftragsmanagement
- ☑ dokumentiertes Verfahren zur Auswahl des Dienstleisters