Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

zwischen

– Verantwortlicher –
(nachfolgend „Auftraggeber“ genannt)

und

AGA Service GmbH
Kurze Mühren 1
20095 Hamburg

– Auftragsverarbeiter –
(nachfolgend „Auftragnehmer“ genannt)

(beide gemeinsam nachfolgend „Vertragsparteien“ genannt)

Präambel

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1 Gegenstand des Auftrags, Art und Zweck der Verarbeitung

(1) Organisatorische Abwicklung von Großkundenabonnents für Unternehmen in der Metropolregion Hamburg und Hannover zur Übermittlung einer HVV- bzw. JobCard-Abonnentenkarten für die jeweiligen Mitarbeiter.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus dem Dienstleistungsvertrag, auf den hier verwiesen wird (im Folgenden „Hauptvertrag“).

Eine Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer ist darüber hinaus nicht vorgesehen.

(3) Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen dokumentierten Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO) und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44-49 DSGVO erfüllt sind.

2 Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

☒ Personenstammdaten

☒ Kommunikationsdaten (Ansprechpartner Personalabteilung)

☒ Vertragsabrechnungs- und Zahlungsdaten Bankverbindung Unternehmen

(2) Kreis der betroffenen Personen:

☒ Kunden (Geschäftskunden)

☒ Mitarbeiter (Mitarbeiter von Kunden)

3 Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

4 Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5 Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind 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.

6 Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

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.

(2) Die Vertragsparteien vereinbaren die in dem **Anlage 1 „Technische und organisatorische Maßnahmen“** zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(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 und dem Auftraggeber schriftlich mitzuteilen.

7 Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. 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 Subunternehmer nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers beauftragen.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die durch den Auftraggeber zum Zeitpunkt des Vertragsschlusses genehmigten Subunternehmer sind in der **Anlage 2** zu diesem Vertrag aufgelistet.

(5) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8 Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9 Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG-neu gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen.

Als externer Datenschutzbeauftragter ist beim Auftragnehmer Herr RA Tim-Oliver Ritz bestellt.

Sie erreichen Ihn unter: zHd Datenschutzbeauftragter, Kurze Mühren 1, 20095 Hamburg, oder per E-Mail an datenschutz@aga.de oder telefonisch 040-308010.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10 Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftragnehmer weist unaufgefordert dem Auftraggeber in Textform mit Datumsangabe nach, dass er sämtliche Datenträger sowie sonstigen Unterlagen an den Auftraggeber herausgegeben oder datenschutzkonform vernichtet oder gelöscht und somit keine Daten des Auftraggebers zurückbehalten hat.

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

11 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme des Auftragnehmers inspizieren.

(2) Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu den üblichen Geschäftszeiten Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Inspektionen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

(3) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

12 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen

Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13 Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1 „Technische und organisatorische Maßnahmen“
- Anlage 2 „Genehmigte Subunternehmer“

Ort, Datum:	
Stempel, Unterschrift Auftraggeber	

Ort, Datum:	Hamburg, den 14.5.2018
AGA Service GmbH	
Stempel, Unterschrift Auftragnehmer	

Anlage 1 Technische und organisatorische Maßnahmen

Ziffer 6 der Vereinbarung zur Auftragsdatenverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

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

Zutrittskontrolle

Zutrittskontrolle **Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.**	**vorhanden** **ja**
Berechtigungsausweise	☒
Elektronische Zutrittscodekarten/ Zutrittstransponder	☒
Zutrittsberechtigungskonzept	☒
Videoüberwachung	☒
Alarmanlage	☒
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Sicherung auch außerhalb der Arbeitszeit durch Werkschutz	☒
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☒
Gesondert gesicherter Zutritt zum Rechenzentrum	☒
Aufbewahrung der Server in verschlossenen Räumen	☒

Zugangskontrolle

Zugangskontrolle **Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.**	**vorhanden** **ja**
Verschlüsselung von Netzwerken (VPN, TLS, Bitlocker)	☒
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☒
Passwortsicherung von Bildschirmarbeitsplätzen	☒
Verwendung von individuellen Passwörtern	☒
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☒

Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☒
Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität:	☒
▪ Mindestens 8 Ziffern / Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)	☒
▪ Verhinderung von Trivialpasswörtern (z.B. Hund1, Hund2, Hund3)	☒
▪ Passworthistorie (keine erneute Verwendung der letzten 5 Passwörter)	☒
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	☒
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☒
Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☒
Verpflichtung zur Vertraulichkeit	☒
Protokollierung und Auswertung der Systembenutzung	☒
Kontrollierte Vernichtung von Datenträgern	☒

Zugriffskontrolle

Zugriffskontrolle **Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.**	**vorhanden** **ja**
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	☒
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Regelmäßige Auswertung von Protokollen (Logfiles)	☒
Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt?	
▪ Virenscanner	☒
▪ Firewalls	☒
▪ SPAM-Filter	☒
▪ Intrusionprevention (IPS)	☒
▪ Intrusiondetection (IDS)	☒
▪ Software für das Security Information and Event Management (SIEM)	☒

Trennungskontrolle

Trennungskontrolle **Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.**	vorhanden ja
Dateiseparierung bei Datenbanken	☒
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☒
Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern des Auftragnehmers	☒
Funktionstrennung	☒
Trennung von Entwicklungs-, Test- und Produktivsystem	☒
Sonstiges: dediziertes System	☒

Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) **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 entsprechende technischen und organisatorischen Maßnahmen unterliegen;**	vorhanden ja
Maßnahmen:	☒

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

Weitergabekontrolle

Weitergabekontrolle **Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.**	**vorhanden** **ja**
Welche Versendungsart der Daten besteht zwischen Auftraggeber und Dritten?	
▪ VPN-Verbindung (IP-Sec)	☒
▪ Datenaustausch über https-Verbindung	☒
▪ Sonstige Versendungsart: ftps	☒
Verschlüsselung vertraulicher Datenträger	☒
Verschlüsselung von Laptopfestplatten	☒

Verschlüsselung mobiler Datenträger	☒
Kontrollierte Vernichtung von Daten:	☒
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	
▪ Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☒
▪ Sonstiges: Überschreibung bei Bändern und Festplatten	☒
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	
▪ Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
▪ Shredder gem. DIN 66399	☒

Eingabekontrolle

Eingabekontrolle **Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten**	**vorhanden** **ja**
Festlegung von Benutzerberechtigungen (Profile)	☒
Differenzierte Benutzerberechtigungen:	☒
Verpflichtung auf die Vertraulichkeit	☒

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

Verfügbarkeitskontrolle

Verfügbarkeitskontrolle **Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.**	**vorhanden** **ja**
Datensicherungs- und Backupkonzepte	☒
Durchführung der Datensicherungs- und Backupkonzepte	☒
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	☒
Rauchmelder in Serverräumlichkeiten	☒
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	☒
Klimatisierte Serverräumlichkeiten	☒
Blitz-/ Überspannungsschutz	☒
Serverräumlichkeiten in separaten Brandabschnitt	☒

Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	☒
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft	☒
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☒
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	☒
Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)	☒
Einbeziehung des Einflusses angrenzender baulicher Einrichtungen	☒
Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)	☒
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☒

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle **Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.**	**vorhanden** **ja**
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot	☒
Festplattenspiegelung	☒
Abgrenzung kritischer Komponenten	☒
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☒
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	☒
Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.	
▪ Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind.	☒
▪ Durchführung einer Risikoanalyse unter Berücksichtigung all dieser Systeme, Geräte und Vermögenswerte, die identifiziert wurden, zur Ermittlung der Bedrohungen, inklusive ihrer Wahrscheinlichkeit und ihrer Auswirkungen.	☒

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

Kontrollverfahren

Kontrollverfahren **Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren**	**vorhanden** **ja**
Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☒
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Es werden datenschutzfreundliche Voreinstellungen gewählt	☒
Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen	☒
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	☒
Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).	☒

Auftragskontrolle

Auftragskontrolle **Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.**	**vorhanden** **ja**
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	☒
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	☒
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒

Anlage 2 Genehmigte Subunternehmer

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Subunternehmer zu, jedoch nur unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO:

Firma (Subunternehmer), Adresse	Verarbeitungsstandort	Art der Dienstleistung
AMCON GmbH, Cloppenburg	Hamburg	Programm zur Erfassung der Unternehmen und deren Mitarbeiter für die Abwicklung der Proficard und Buchhaltung
S-Bahn Hamburg GmbH	Hamburg	Mahnverfahren für säumige Teilnehmer
GVH Großraum-Verkehr Hannover GmbH	Hannover	Zuarbeiten zum Vertragsverhältnis (z.B. Drucken der Fahrkarten, Ersatzfahrausweise)