Vertrag zur Auftragsverarbeitung
Technische und Organisatorische Maßnahmen

Digitales Schwarzes Brett (DSB)

Nach EU-Datenschutz-Grundverordnung (EU-DSGVO)

Zwischen

Heinrich-Hansjakob-Bildungszentrum HAslach
[redacted]
Richard-Wagner-Str. 10
77716 Haslach im Kinzigtal

-nachfolgend AUFTRAGGEBER genannt-

Und

heinekingmedia GmbH
Hamburger Allee 2-4
30161 Hannover

-nachfolgend AUFTRAGNEHMER genannt-

Präambel
Diese Datenschutzvereinbarung findet Anwendung auf alle Tätigkeiten des AUFTRAGNEHMERS im Rahmen des zwischen den Parteien geschlossenen Digitales Schwarzes Brett- Bereitstellungsvertrages (nachstehend „Hauptvertrag“) bei denen der AUFTRAGNEHMER bzw. seine Mitarbeiter und/oder Erfüllungsgehilfen personenbezogene Daten des AUFTRAGGEBERS i. S. d. EU-Datenschutzgrundverordnung (EU-DSGVO) sowie spezialgesetzlicher Vorschriften verarbeiten oder mit diesen in Berührung kommen, so dass regelmäßig der Tatbestand der Auftragsverarbeitung gemäß Art. 28 EU-DSGVO erfüllt ist.
Der AUFTRAGGEBER hat den AUFTRAGNEHMER im Rahmen seiner Sorgfaltspflichten als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der AUFTRAGGEBER dem AUFTRAGNEHMER den Auftrag schriftlich erteilt. Diese Datenschutzvereinbarung enthält nach dem Willen der Parteien und insbesondere der AUFTRAGGEBER den schriftlichen Auftrag i. S. d. Art. 28 Abs. 3 EU-DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.
Sofern in dieser Datenschutzvereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst

insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung oder sonstige Nutzung von Daten.

1. **§1 Gegenstand des Auftrags**
    1. Verschlüsselte, über eine Authentifizierung geschützte Übertragung von digitalen Aushängen, Vertretungslisten und Newsticker-Nachrichten sowie Verteilung diverser vom Auftraggeber ausgewählter, erstellter oder erzeugter Daten und Informationen an frei zugängliche Displays und mobile Endgeräte für folgende Zwecke:
        - Benachrichtigen und Informieren von Empfängern (Lehrer, Schüler, Mitarbeiter, Lehrern oder sonstigen vom Auftraggeber ausgewählten Empfängern.
    2. Verschlüsselter und über Authentifizierung möglicher Abruf der o.a. Daten zur Anzeige auf Digitalen Schwarzen Brettern (DSBs), passwortgeschützt auf der Schul-/ Firmeninternetseite (netschool/netbizz DSBmobile), Ausgabe auf einer dezidierten und passwortgeschützten Smartphone-App (netschool/netbizz DSBmobile).
    3. Der AUFTRAGGEBER ist im Rahmen dieser Datenschutzvereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den AUFTRAGNEHMER sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle i. S. d. Art. 4 Abs. 8 EU-DSGVO).
    4. Aufgrund der vorstehend genannten Verantwortlichkeit kann der AUFTRAGGEBER auch während der Laufzeit des Hauptvertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.
2. **§ 2 Umfang der Weisungsbefugnisse des AUFTRAGGEBERS**
    1. Der AUFTRAGNEHMER verarbeitet personenbezogene Daten des AUFTRAGGEBERS ausschließlich im Rahmen der vertraglichen Vereinbarungen und Weisungen des AUFTRAGGEBERS.
       Ohne einen entsprechenden Auftrag bzw. einer Weisung des AUFTRAGGEBERS ist der Zugriff des AUFTRAGNEHMERS auf Daten des AUFTRAGGEBERS grundsätzlich nicht gestattet. Sollte im Einzelfall der Zugriff auf Daten des AUFTRAGGEBERS erforderlich sein, ist vorab die Einwilligung des AUFTRAGGEBERS in Schriftform oder Textform (z.B. E-Mail) einzuholen. Sollte aufgrund von Eilbedürftigkeit (z.B. Gefahr in Verzug) eine solche vorherige Einwilligung des AUFTRAGGEBERS nicht vorher eingeholt werden können, wird der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich nach Beendigung der jeweiligen Maßnahme informieren.
    2. Der AUFTRAGGEBER hat das Recht, jederzeit ergänzende (Einzel-)Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den AUFTRAGNEHMER zu erteilen. Der AUFTRAGGEBER wird dem AUFTRAGNEHMER eine angemessene Frist zur Umsetzung der Weisungen setzen.
       Die Weisungsgebundenheit des AUFTRAGNEHMERS erstreckt sich auch auf die notwendige Mitwirkung bei der Erstellung des Verarbeitungsverzeichnisses und bei den dem AUFTRAGGEBER obliegenden Zulässigkeits- und Ordnungsmäßigkeitskontrollen. Die Weisungen des AUFTRAGGEBERS bedürfen der Schrift- oder Textform. Mündliche Weisungen sind vom AUFTRAGGEBER schriftlich oder in Textform zu bestätigen.

3. Der AUFTRAGGEBER und der AUFTRAGNEHMER benennen schriftlich oder in Textform jeweils einen Ansprechpartner, der zur Abgabe von (Einzel-)Weisungen bzw. für die Annahme von (Einzel-) Weisungen im Zusammenhang mit der vertragsgegenständlichen Datenverarbeitung berechtigt ist.
   Bei einem Wechsel oder einer dauerhaften Verhinderung des verantwortlichen Ansprechpartners ist dies durch den jeweiligen Vertragspartner unverzüglich schriftlich oder in Textform unter Benennung eines Vertreters mitzuteilen.
4. Ist der AUFTRAGNEHMER der Ansicht, dass eine Weisung des AUFTRAGGEBERS gegen die EU-DSGVO oder andere datenschutzrechtliche Vorschriften verstößt, hat er den AUFTRAGGEBER unverzüglich darauf hinzuweisen.
5. Erteilt der AUFTRAGGEBER (Einzel-)Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten durch den AUFTRAGGEBER zu tragen.

3. **§3 Pflichten des AUFTRAGNEHMERS**
   1. Der AUFTRAGNEHMER wird die für den Datenschutz und die Datenverarbeitung vertraglich vereinbarten und für ihn gesetzlich geltenden Vorschriften beachten. Die entsprechenden Pflichten des AUFTRAGNEHMERS im Zusammenhang mit der Datenverarbeitung im Auftrag, einschließlich der von dem AUFTRAGNEHMER durchzuführenden Kontrollen, sind im Einzelnen in Art. 32 Abs. 1 EU-DSGVO aufgeführt.
   2. Der AUFTRAGNEHMER verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des AUFTRAGGEBERS.
   3. Der AUFTRAGNEHMER stellt i. S. d. Art. 32 Abs. 4 EU-DSGVO sicher, dass alle Schritte zur Verarbeitung von personenbezogenen Daten von dem AUFTRAGGEBER nur auf Anweisung durch den Verantwortlichen unternommen werden, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.
   4. Bei der Verarbeitung von Daten achtet der AUFTRAGNEHMER insbesondere darauf, dass ggf. eine vom AUFTRAGGEBER angeforderte Berichtigung, Sperrung und Löschung personenbezogener Daten durchgeführt wird.
   5. Der AUFTRAGNEHMER stellt dem AUFTRAGGEBER die für die Übersicht nach Art. 30 DSGVO; sowie für die Durchführung der Folgenabschätzung nach Art. 35 DSGVO erforderlichen Angaben zur Verfügung.
   6. Der AUFTRAGNEHMER unterrichtet den AUFTRAGGEBER unverzüglich über Verstöße gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des AUFTRAGGEBERS, die im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt oder dem AUFTRAGNEHMER in sonstiger Weise bekannt geworden sind.
      Ebenso benachrichtigt der AUFTRAGNEHMER den AUFTRAGGEBER umgehend bei Störungen des Betriebsablaufes bzw. Verarbeitungsablaufs, Verlust oder Beschädigung von Datenträgern und anderen Unregelmäßigkeiten bei der Verarbeitung der Daten.
   7. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien wird der AUFTRAGNEHMER erst nach entsprechender (Einzel-)Weisung des AUFTRAGGEBERS datenschutzgerecht vernichten. Ggf. vom

AUFTRAGGEBER überlassene Datenträger sind an den AUFTRAGGEBER auf Anforderung zurückzugeben.

4. **§ 4 Pflichten des AUFTRAGGEBERS**
    1. Der AUFTRAGGEBER ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.
    2. Der AUFTRAGGEBER hat den AUFTRAGNEHMER unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
    3. Die Pflicht zur Führung des öffentlichen Verarbeitungsverzeichnisses gem. Art. 30 EU-DSGVO liegt bei dem AUFTRAGGEBER.
5. **§ 5 Technische und organisatorische Maßnahmen zur Datensicherheit**
    1. Der AUFTRAGNEHMER wird in seinem Verantwortungsbereich die vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 32 Abs. 1 EU-DSGVO umsetzen und einhalten. Insbesondere wird der AUFTRAGNEHMER seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des AUFTRAGGEBERS vor Missbrauch und Verlust treffen, die den Forderungen des EU-DSGVO entsprechen. Dies beinhaltet insbesondere
        1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
        2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
        3. dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung 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 (Zugriffskontrolle),
        4. dafür Sorge zu tragen, 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 (Weitergabekontrolle),
        5. dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
        6. dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AUFTRAGGEBERS verarbeitet werden können (Auftragskontrolle),
        7. dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
        8. dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

2. Die Parteien haben die hiernach im Einzelnen zu treffenden Maßnahmen in der Anlage (Anhang B, Vereinbarung zur Auftragsverarbeitung nach Art. 32 Abs. 1 EU-DSGVO, Technische und organisatorische Maßnahmen) zu dieser Vereinbarung, die Vertragsbestandteil wird, gesondert festgeschrieben.

6. **§ 6 Kontrollrechte des AUFTRAGGEBERS**
    1. Der AUFTRAGGEBER hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des AUFTRAGGEBERS durch den AUFTRAGNEHMER jederzeit im erforderlichen Umfang zu kontrollieren. Die Durchführung einer Kontrolle in den Geschäftsräumen des AUFTRAGNEHMERS ist nur nach vorheriger schriftlicher Ankündigung mit angemessener Frist und nur zu den üblichen Geschäftszeiten des AUFTRAGNEHMERS zulässig.
    2. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER auf Anforderung innerhalb einer angemessenen Frist alle Auskünfte geben, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.
7. **§ 7 Unterauftragsverhältnisse**
    1. Der AUFTRAGGEBER ist damit einverstanden, dass der AUFTRAGNEHMER zur Erfüllung seiner vertraglich vereinbarten Leistungen den Subunternehmer Mivitec GmbH, Wamslerstr. 4 - 81829 München beauftragt.
    2. Erteilt der AUFTRAGNEHMER Aufträge an Subunternehmer, so obliegt es dem AUFTRAGNEHMER, seine Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieser Datenschutzvereinbarung. Der AUFTRAGNEHMER stellt dabei sicher, dass die als Subunternehmer beauftragten Unternehmen der EU-Datenschutzrichtlinie unterfallen. Der Subunternehmer unterliegt der Kontrolle des AUFTRAGGEBERS.
    3. Der AUFTRAGNEHMER wird den Subunternehmer sorgfältig auswählen und vor der Beauftragung prüfen, ob dieser die zwischen dem AUFTRAGGEBER und dem AUFTRAGNEHMER getroffenen Vereinbarungen einhalten kann.
    4. Der AUFTRAGNEHMER wird zudem vor Beauftragung und in regelmäßigen Abständen während der Vertragsdauer kontrollieren, ob der Subunternehmer die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.
8. **§ 8 Wahrung der Betroffenenrechte**
    1. Der AUFTRAGGEBER ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der AUFTRAGNEHMER ist nicht berechtigt, Dritten – aber auch den Betroffenen selbst – Auskünfte im Hinblick auf personenbezogene Daten zu erteilen. Auskunftsersuchen Betroffener wird der AUFTRAGNEHMER unverzüglich an den AUFTRAGGEBER bzw. den Datenschutzbeauftragten des AUFTRAGGEBERS weiterleiten.
    2. Ist der AUFTRAGGEBER aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der AUFTRAGNEHMER den AUFTRAGGEBER dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt
        0. Der AUFTRAGGEBER hat den AUFTRAGNEHMER hierzu schriftlich oder in Textform aufgefordert und

1. 8.2.b) Der AUFTRAGGEBER erstattet dem AUFTRAGNEHMER die durch diese Unterstützung entstandenen Kosten.

9. **§ 9 Laufzeit**

Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages.

10. **§ 10 Löschungen von Daten und Rückgabe von Datenträgern**
    1. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des AUFTRAGGEBERS. Der AUFTRAGNEHMER hat diese sorgfältig zu verwahren, sodass sie Dritten nicht zugänglich sind.
    2. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der AUFTRAGNEHMER auf Grund einer Einzelbeauftragung durch den AUFTRAGGEBER. In besonderen, vom AUFTRAGGEBER zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe durch den AUFTRAGNEHMER.
    3. Der AUFTRAGGEBER legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung eines Auftrags (Leistungsschein) oder des Hauptvertrags vertraglich oder durch (Einzel-)Weisung in Schrift- oder Textform fest.
    4. Entstehen zusätzliche Kosten durch die Herausgabe oder Löschung von Daten, so trägt diese der AUFTRAGGEBER.
11. **§ 11 Schlussbestimmungen**
    1. Sollten die Daten des AUFTRAGGEBERS beim AUFTRAGNEHMER durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich darüber zu informieren. Der AUFTRAGNEHMER wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten bei dem AUFTRAGGEBER liegt.
    2. Diese Vereinbarung unterliegt dem für Rechtsbeziehungen unter Inländern maßgeblichen Recht der Bundesrepublik Deutschland.
    3. Gerichtsstand für alle sich aus oder im Zusammenhang mit dieser Vereinbarung ergebenden Streitigkeiten ist, soweit es sich bei dem Vertragspartner um einen Kaufmann im Sinne des Handelsgesetzbuchs, eine juristische Person des öffentlichen Rechts oder ein öffentlich- rechtliches Sondervermögens handelt, Hannover. Der AUFTRAGNEHMER ist in diesem Fall jedoch auch berechtigt, vor dem für den AUFTRAGGEBER örtlich zuständigen Gericht Klage zu erheben.
    4. Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Einhaltung der gesetzlichen der Schriftform, soweit gesetzlich keine strengere, insbesondere notarielle Form vorgeschrieben ist. Dies gilt auch für einen Verzicht auf das vorstehende Schriftformerfordernis. Mündliche Nebenabreden sind nicht getroffen.

Anhang
zum Vertrag zur Auftragsverarbeitung gem. Art. 32 Abs. 1 EU-DSGVO
- Technische und organisatorische Maßnahmen -

§ 1 Anwendungsbereich

Die nachstehend beschriebenen technischen und organisatorischen Maßnahmen (TOM)

dienen dem Schutz personenbezogener Daten und werden von MIVITEC unabhängig von darüberhinausgehenden Anforderungen aus Verträgen zugesichert.

§ 2 Zutrittskontrolle
Die Maßnahmen der Zutrittskontrolle verhindern den körperlichen Zutritt Unbefugter zu den Datenverarbeitungsanlagen, auf denen personenbezogen Daten verarbeitet werden („Datenverarbeitungssysteme“)
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Mehrfaktorauthentifizierung
  Der Zutritt zu den Datenverarbeitungssystemen ist nur nach erfolgreicher Authentifizierung anhand von mindestens zwei Faktoren unterschiedlichen Typs (z. B. biometrisches Merkmal und PIN) möglich.
- Zutrittsprotokollierung
  Jeder Zutritt zu Sicherheitsbereichen, in denen sich Datenverarbeitungssysteme befinden, wird automatisch protokolliert und kann daher nachvollzogen werden.
- Videoüberwachung
  Sicherheitsbereiche, in denen sich Datenverarbeitungssysteme befinden, werden permanent von Videokameras überwacht. Die Aufnahmen werden gespeichert und für einen angemessenen Zeitraum aufbewahrt.
- Versperrte Racks
  Racks, in denen sich Datenverarbeitungssysteme befinden, sind versperrt. Die Schlüssel werden zentral verwaltet.
- Fluchttüren
  Sicherheitsbereiche dürfen ausschließlich durch die dafür vorgesehenen Eingänge betreten werden. Fluchttüren können von außen nicht als Eingang benutzt werden. Das Öffnen von Fluchttüren führt zu einer Alarmierung.
- Genehmigungspflicht
  Zutrittsberechtigungen zu den Sicherheitsbereichen unterliegen einem formalisierten Genehmigungsverfahren.
- Reinigungs- und Wartungsarbeiten
  In Sicherheitsbereichen finden keine unbegleiteten Wartungs- oder Reinigungsarbeiten durch Unberechtigte statt.

§ 3 Zugangskontrolle
Die Maßnahmen der Zugangskontrolle verhindern die Nutzung von Datenverarbeitungsanlagen auf denen personenbezogene Daten durch Unbefugte.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Genehmigungspflicht
  Zugangsberechtigungen zu den Datenverarbeitungssystemen unterliegen einem formalisierten Genehmigungsverfahren.
- Passwörter
  Der Zugang zu Datenverarbeitungssystemen ist nur nach vorheriger Authentifizierung anhand von Benutzernamen und Passwörtern möglich. Die Mindestanforderungen an Passwortlänge- und -komplexität sowie der Umgang mit Passwörtern sind in einer Richtlinie definiert und werden systemseitig unterstützt. Passwörter werden mit Zufallsgeneratoren erzeugt. Passwörter werden in Anmeldeverfahren verschlüsselt übertragen.
- Protokollierung
  Jede Anmeldung an einem Datenverarbeitungssystem wird protokolliert. Die

Protokolle sind gegen Veränderung geschützt und werden für einen angemessenen Zeitraum aufbewahrt.

- Verschlüsselung
  Kommen mobile Geräte wie z. B. Notebooks zum Einsatz, so werden deren Festplatten mit einer angemessenen Methode Verschlüsselt.
- Mobile Datenträger
  Personenbezogene Daten werden nicht auf mobilen Datenträgern wie z. B: USB-Sticks oder DVDs gespeichert.
- Aufgabentrennung
  An der Verwaltung der Datenverarbeitungssysteme und deren Infrastruktur sind verschiedene Mitarbeiter beteiligt, deren Verantwortlichkeiten und Berechtigungen in einem Rollenkonzept geregelt sein.
- Regelmäßige Überprüfung
  Im Rahmen von internen Audits werden regelmäßig Zugangsberechtigungen zu Datenverarbeitungssystemen kontrolliert und auf ihre Rechtmäßigkeit geprüft.
- Screenlock
  Arbeitsstationen der Mitarbeiter sind so konfiguriert, dass nach Ablauf eines Zeitintervalls der passwortgeschützte Bildschirmschoner aktiviert wird.

§ 4 Zugriffskontrolle

Die Maßnahmen der Zugriffskontrolle stellen sicher, dass berechtigte Benutzer der Datenverarbeitungssysteme ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und das Unberechtigte Daten weder lesen, kopieren, verändern oder löschen können.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Genehmigungspflicht
  Zugriffsberechtigungen zu den Datenverarbeitungssystemen unterliegen einem formalisierten Genehmigungsverfahren.
- Entzug von Berechtigungen
  Bei der Beendigung oder Veränderung der Anstellung von Mitarbeitern werden nicht mehr benötigte Zugriffsberechtigungen entzogen.
- Passwörter
  Der Zugriff auf personenbezogene Daten ist nur nach vorheriger Authentifizierung anhand von Benutzernamen und Passwörtern möglich. Die Mindestanforderungen an Passwortlänge- und -komplexität sowie der Umgang mit Passwörtern sind in einer Richtlinie definiert und werden systemseitig unterstützt. Passwörter werden mit Zufallsgeneratoren erzeugt. Passwörter werden in Anmeldeverfahren werden verschlüsselt übertragen.
- Verschlüsselung
  Kommen mobile Geräte wie z. B. Notebooks zum Einsatz, so werden deren Festplatten mit einer angemessenen Methode Verschlüsselt.
- Mobile Datenträger
  Personenbezogene Daten werden nicht auf mobilen Datenträgern wie z. B: USB-Sticks oder DVDs gespeichert.
- Zugriffsprotokollierung
  Jeder Zutritt zu Sicherheitsbereichen, in denen sich Datenverarbeitungssysteme befinden, wird automatisch protokolliert und kann daher nachvollzogen werden.
- Bildschirmsperre
  Arbeitsstationen der Mitarbeiter sind so konfiguriert, dass nach Ablauf eines Zeitintervalls die passwortgeschützte Bildschirmsperre aktiviert wird.

§ 5 Weitergabekontrolle
Der Maßnahmen der Weitergabekontrolle verhindern, dass Datenträger durch Unbefugte gelesen, kopiert, verändert oder gelöscht werden können. Darüber hinaus fallen hierunter auch jene Maßnahmen, die personenbezogene Daten bei der Übertragung durch Netzwerke schützen.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Verschlüsselung
  Personenbezogene Daten werden nur verschlüsselt (TLS) übertragen. Kommen mobile Geräte wie z. B. Notebooks zum Einsatz, so werden deren Festplatten mit einer angemessenen Methode Verschlüsselt.
- Datenträger
  Physikalische Datenträger werden nicht versandt.
- Fernwartung
  Fernwartungen erfolgen ausschließlich mittels verschlüsselter Kommunikation und unter Verwendung von eigenen Systemen durch eigene Mitarbeiter statt.
- Protokollierung
  Daten zu Verbindungen werden protokolliert und sind gegen Veränderungen geschützt. Die Aufbewahrung erfolgt für einen angemessenen Zeitraum.

§ 6 Eingabekontrolle
Die Maßnahmen der Eingabekontrolle stellen sicher, dass jederzeit festgestellt werden welche personenbezogenen Daten zu welcher Zeit von wem im Datenverarbeitungssystem eingegeben, verändert oder gelöscht wurden.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Genehmigungspflicht
  Zugriffsberechtigungen zu den Datenverarbeitungssystemen unterliegen einem formalisierten Genehmigungsverfahren.
- Protokollierung
  Jeder Systemzugriff wird protokolliert. Die Protokolle sind gegen Veränderung geschützt und werden für einen angemessenen Zeitraum aufbewahrt.
- Klassifizierung
  Eine Richtlinie regelt die Klassifizierung von Datenarten wie z. B. personenbezogenen Daten.

§ 7 Auftragskontrolle
Die Maßnahmen der Auftragskontrolle stellen sicher, dass die von der MIVITEC GmbH im Auftrag verarbeiteten personenbezogenen Daten entsprechend den Weisungen des Auftraggebers verarbeitet werden. Darüber hinaus fallen hierunter auch jene Maßnahmen, die zu ergreifen sind, falls relevante Subunternehmer eingesetzt werden.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- ADV-Vertrag
  Verarbeitet die MIVITEC GmbH personenbezogene Daten im Auftrag Dritter, wird hierfür ein Vertrag zur Auftragsverarbeitung (ADV-Vertrag) mit dem Auftraggeber vereinbart, indem die Rechte und Pflichten der beteiligten Parteien geregelt sind.
- Unterauftragnehmer
  Im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag von Kunden kommen keine Unterauftragnehmer im datenschutzrechtlichen Sinne zum Einsatz, wenn dies nicht mit dem Auftraggeber vereinbart ist. Ist der Einsatz

vereinbart, so werden zukünftige Unterauftragnehmer erst auf ihre Eignung hin überprüft.

- ADV-Vertrag
  Kommt ein Unterauftragnehmer zum Einsatz. So werden Rechte und Pflichten in einem ADV-Vertrag geregelt.
- Überwachung
  Alle sicherheits/datenschutzrelevanten Auftragnehmer der MIVITEC GmbH werden regelmäßig auditiert um die Einhaltung der vereinbarten Maßnahmen zu prüfen.

§ 8 Verfügbarkeitskontrolle

Die Maßnahmen der Verfügbarkeitskontrolle stellen den Schutz der personenbezogenen Daten vor zufälliger Zerstörung z. B. durch Feuer sicher.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Brandschutz
  Rechenzentren sind mit angemessenen Systemen zur Erkennung von Bränden und Alarmierungssystemen ausgestattet. In kritischen Sicherheitsbereichen stehen automatische Löschanlagen zur Verfügung. Sicherheitsbereiche werden regelmäßig auf vermeidbare Brandlasten hin überprüft.
- Stromversorgung
  Die Stromversorgung erfolgt aus einer ausfallsicheren Ringleitung. Die Rechenzentren verfügen über eine Anlage zur unterbrechungsfreien Stromversorgung (USV), die den Weiterbetrieb der Datenverarbeitungssysteme bei Ausfall der Stromzuführung gewährleistet. Kritische Sicherheitsbereiche sind darüber hinaus mit einer Netzersatzanlage (NEA) ausgestattet, die eine eigenständige Stromversorgung auch über längere Zeiträume hinweg gewährleistet.
- Klimaversorgung
  Die Gewährleistung der geeigneten Temperatur und Luftfeuchtigkeit in den Rechenzentren wird über redundante Klimageräte sichergestellt.
- Netzwerkanbindung
  Die vereinbarte Anbindung von Datenverarbeitungssystemen an vereinbarte Netzwerke erfolgt über redundante Leitungen verschiedener Anbieter.
- Datensicherung
  Datenverarbeitungssysteme, deren Betrieb von der MIVITEC GmbH verantwortet, werden mindestens einmal täglich inkrementell und mindestens einmal wöchentlich vollumfänglich an einen anderen Standort gesichert.
- Notfallplanung
  Die MIVITEC GmbH verfügt über umfangreiche Notfallkonzepte für alle Rechenzentren, die regelmäßig erprobt werden.

§ 9 Trennungsgebot

Die Maßnahmen des Trennungsgebots stellen sicher, dass die personenbezogenen Daten vereinbarungsgemäß von anderen Datenverarbeitungssysteme logisch oder physisch getrennt sind und keine unerlaubte Zusammenführung mit anderen Daten stattfindet.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Mandantentrennung
  Datenverarbeitungssysteme verschiedener Auftraggeber werden physisch oder logisch so voneinander getrennt, dass eine gegenseitige unberechtigte Einsichtnahme ausgeschlossen ist.

- Entwicklungs- und Testumgebung
  Die MIVITEC GmbH führt Entwicklungs- und Testaufgaben ausschließlich in hierfür vorgesehenen Entwicklungs- und Testumgebungen durch.

§ 10 Organisationskontrolle
Die Maßnahmen der Organisationskontrolle stellen sicher, dass die für den Umgang mit personenbezogenen Daten erforderliche organisatorischen Ressourcen und Regelungen zur Verfügung stehen.
Zu diesem Zweck sind die folgenden Maßnahmen umgesetzt:

- Datenschutzbeauftragter
  Die MIVITEC GmbH hat einen fachkundigen externen Datenschutzbeauftragten bestellt; Name und Kontaktinformationen sind dem Verfahrensverzeichnis zu entnehmen.
- Datenschutzkonzept
  Der Umgang mit personenbezogenen Daten ist in einem für alle Mitarbeiter verbindlichen Datenschutzkonzept geregelt.
- Verpflichtungserklärung
  Alle Mitarbeiter sind auf das Datengeheimnis gem. § 5 BDSG, § 35 SGB I und § 80 SGB X und § 88 TKG verpflichtet.
- Schulung
  Alle Mitarbeiter werden regelmäßig von einem fachkundigen Datenschutzexperten im Umgang mit personenbezogenen Daten geschult.
- Regelmäßige Überprüfung
  Sämtliche Maßnahmen zum Datenschutz werden im Rahmen von internen Audits regelmäßig überprüft.

Dieses Dokument wurde von Christof Terglane am 28.06.2018 12:35:00 digital bestätigt.

Dieses Schreiben wurde maschinell erstellt und ist daher ohne Unterschrift gültig.