Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftragsdatenverarbeiter]

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN GEMÄß ART 25 EU-DSGVO/DER ANLAGE ZU § 9 BDSG A.F.

1 Zutrittskontrolle

1.1 Die Räumlichkeiten von [ABC] in denen Kunden-Daten erhoben, verarbeitet und/oder genutzt werden, werden ausschließlich von Mitarbeitern und entsprechend dieser Bestimmungen verpflichteten Vertragspartnern von [ABC] genutzt und betreten. Ausgenommen hiervon sind Personen, die sich zur Erfüllung der Verpflichtungen aus dem Rahmenvertrag in den Räumlichkeiten aufhalten müssen und die dabei während ihres gesamten Aufenthalts von Zutrittsberechtigten im Sinne des Satz 1 dieser Ziffer 1.1 begleitet werden.

1.2 Die Eingänge zu den Räumlichkeiten sind mit Sicherheitsschlüsseln sowie Magnetkartenschlössern gegen Zutritt Unbefugter gesichert.

1.3 Türen, Tore und Fenster werden außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster in Keller und Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu den Räumen sind derart gesichert, dass diese Unbefugten nur erheblich erschwert zugänglich sind.

1.4 Die Vergabe von Zutrittsberechtigungen und von Schlüsseln, Magnetkarten, und Ausweisen ist nachvollziehbar dokumentiert. Das Betreten der Räumlichkeiten wird unverzüglich beim Betreten und für jeweils einen Zeitraum von einem Monat nach Betreten der Räumlichkeiten protokolliert.

1.5 Soweit von [ABC] Kunden-Daten auf selbst oder von Dritten betriebenen Servern erhebt, verarbeitet und/oder nutzt, ist dieser Server in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, die durch eine Zutrittskontrollanlage geschützt sind. Der Zutritt ist nur befugten Mitarbeitern in dem zur Leistungserbringung erforderlichen Umfang gestattet und wird unverzüglich beim Betreten und für jeweils einen Zeitraum von einem Monat nach Betreten der Räumlichkeiten protokolliert. Die Protokolle werden regelmäßig stichprobenartig überprüft.

1.6 Sämtliche Dokumente und Datenträger, die Kunden-Daten enthalten (einschließlich sämtliche Sicherungskopien von Kunden-Daten und Kopien von Originaldokumenten) sind ständig in verschlossenen Sicherungsschränken aufbewahrt. Der Zugriff ist ausschließlich den zum Zweck der Vertragserfüllung eingesetzten Mitarbeitern von [ABC] möglich.

2 Zugangskontrolle

2.1 Die zur Erhebung, Verarbeitung und/oder Nutzung von Kunden-Daten eingesetzten Systeme von [ABC] sind durch Authentifikations- und Autorisationssysteme geschützt. Dabei verpflichtet sich [ABC] mindestens Benutzerkennungen und komplexe Passwörter gemäß den Bestimmungen der Ziffer 2.6 sowie abgestufte Zugriffsrechte gemäß den Bestimmungen der Ziffer 3 zu verwenden.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftragsdatenverarbeiter]

2.2 [ABC] verpflichtet sich, die Zugangsberechtigungen zu den zur Erhebung, Verarbeitung und Nutzung der Kunden-Daten eingesetzten Systemen (insbesondere in Form von Benutzernamen und Passwörtern) nur an die zur Leistungserbringung eingesetzten Mitarbeiter in dem für die jeweilige Aufgabe erforderlichen Umfang zu vergeben.

2.3 Alle Zugänge sind personenspezifisch zu vergeben. Die Benutzung von Kennungen (Accounts) durch mehrere Personen hat grundsätzlich zu unterbleiben. Ist die Benutzung von Gruppenkennungen unvermeidbar, so muss die Kennung zu jedem Zeitpunkt einer verantwortlichen natürlichen Person zuordenbar sein.

2.4 Soweit zu Zwecken der technischen Wartung Dritte Zugriff auf die Systeme des Auftragnehmers erhalten, sind diese Zugänge derartig eingeschränkt, dass sie keinen Zugriff auf Kunden-Daten ermöglichen. Ausnahmen bedürfen der schriftlichen Genehmigung durch den Auftraggeber.

2.5 Jede Vergabe von Zugängen und Zugriffsberechtigungen ist dokumentiert.

2.6 Bei Verwendung von Passwörtern ist [ABC] verpflichtet, Passwörter in ausreichender Komplexität und Güte zu wählen. Ausreichende Komplexität und Güte bedeutet dabei mindestens eine Länge von acht (8) Zeichen, keine Verwendung generischer Begriffe oder von Eigennamen, sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter.

2.7 Passwörter sind durch den Besitzer der zugehörigen Kennung persönlich zu vergeben und spätestens alle drei (3) Monate durch diesen zu ändern. Dieser Vorgang ist technisch oder organisatorisch zu erzwingen. Bei mehr als drei (3) Fehleingaben eines Passwortes in Folge ist der Zugang zu sperren und nur nach einer erneuten Prüfung der Zugangsberechtigung wieder freizugeben.

2.8 Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) werden streng geheim gehalten und gegenüber unbefugten Dritten nicht bekannt gegeben.

2.9 Sofern Authentifikationsdaten im begründeten Einzelfall aus technischen oder organisatorischen Gründen nicht verschlüsselt übertragen werden können (z.B. für Initialpasswörter oder Passwort-Zurücksetzungen), sind Einweg-Passwörter zu verwenden. Hierbei ist technisch sicherzustellen, dass die übermittelten Passwörter unmittelbar nach der Verwendung geändert werden müssen. Der Auftragnehmer hat sicherzustellen dass die Authentifikationsdaten ausschließlich an zuvor authentifizierte berechtigte Empfänger übermittelt werden.

2.10 [ABC] verpflichtet sich, Netze mit unterschiedlichen Verwendungszwecken und/oder Sicherheitsniveaus durch Firewalls zu trennen sowie diese Firewalls unverzüglich an neue technische Entwicklungen anzupassen. [ABC] hat dabei insbesondere sicherzustellen, dass jede Firewall zumindest eine zustandsgesteuerte und regelbasierte Paketfilterung umsetzt und dass der zur Anwendung kommende Regelsatz die Kommunikation von und zu den Systemen, mit welchen Kunden-Daten erhoben, verarbeitet und/oder genutzt werden, mittels expliziter Freigaben ("Whitelist") auf die minimal für den Betrieb dieser Systeme notwendigen Verbindungen einschränkt. Sämtliche nachträgliche Änderungen an der Konfiguration der Firewall und/oder dem zur Anwendung kommenden Regelsatz sind unter strikter Beachtung einer Rollentrennung ("4-Augen-Prinzip") vorab zu genehmigen und dauerhaft und nachvollziehbar zu dokumentieren.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

2.11 Soweit [ABC] Kunden-Daten auf selbst oder von Dritten betriebenen Servern erhebt, verarbeitet und/oder nutzt, ist dieser Server durch eine Firewall gegen nicht betriebsnotwendige Zugriffe zu sichern.

2.12 [ABC] verpflichtet sich, auf allen zur Erhebung, Verarbeitung und/oder Nutzung von Kunden-Daten eingesetzten Systemen speicherresidente Virenscanner mit mindestens täglichen Updates sowie eine Personal Firewall einzusetzen. Für nach Ziffer 2.1110 dieses Anhangs abgesicherte Server ist keine zusätzliche Personal Firewall notwendig.

3 Zugriffskontrolle

3.1 [ABC] hat für sämtliche Zugriffe auf Kunden-Daten ein abgestuftes und geeignetes Rechtesystem eingerichtet und technisch dauerhaft implementiert. Ein geeignetes Rechtesystem liegt vor, wenn die Zugriffsrechte so gestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten Mitarbeitern jeweils für die Erfüllung der konkreten Aufgaben notwendigen Umfang Zugriff auf die Kunden-Daten erlauben. Die Rechte müssen dabei durch eine auf das zwingend erforderliche Maß begrenzte Anzahl an Mitarbeitern des Auftragnehmers mit Administratorenrechten vergeben und verwaltet werden.

3.2 Der Zugriff auf Kunden-Daten (einschließlich der Eingabe, Veränderung und/oder Löschung) ist vom Auftragnehmer durch die zur Datenverarbeitung eingesetzten Systeme nach Benutzer, Datum, Uhrzeit und den jeweils betroffenen Kunden-Daten mindestens für die Dauer von drei (3) Monaten in Textform zu protokollieren.

3.3 Bei allen zur Erhebung, Verarbeitung und/oder Nutzung von Kunden-Daten eingesetzten Systemen ist eine Nutzung von Kennungen durch andere Personen als den berechtigen Nutzer zu verhindern. [ABC] stellt sicher, dass Systeme, die einen Zugriff auf Kunden-Daten ermöglichen, bei jedem Verlassen der Systeme zumindest durch einen passwortgeschützten Bildschirmschoner vor unberechtigten Zugriffen geschützt sind. [ABC] verpflichtet sich, den Bildschirmschoner bei Inaktivität des angemeldeten Benutzers spätestens nach zehn (10) Minuten automatisch zu aktivieren.

4 Weitergabekontrolle

4.1 [ABC] stellt sicher, dass Kunden-Daten nicht unbefugt kopiert weitergegeben und/oder gelöscht werden können.

4.2 Die mit der Erhebung, Verarbeitung und/oder Nutzung von Kunden-Daten befassten Mitarbeiter dürfen nicht über Administratorenrechte für die zur Erhebung, Verarbeitung und/oder Nutzung von Kunden-Daten eingesetzten Systeme verfügen.

4.3 [ABC] stellt sicher, dass auf Systemen, mit denen Kunden-Daten erhoben, verarbeitet und/oder genutzt werden, keine Software eingesetzt wird, bei der nicht durch eine aktive Kontrollmöglichkeit durch [ABC] ausgeschlossen ist, dass diese Software Kunden-Daten an Dritte übermittelt.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftragsdatenverarbeiter]

5 Eingabekontrolle

[ABC] stellt bis zur Löschung der Kunden-Daten durch dauerhafte Protokollierung und organisatorische Maßnahmen sicher, dass auf Verlangen des Auftraggebers jederzeit, auch nachträglich, zuverlässig festgestellt werden kann ob, wann, wo und von wem Kunden-Daten erhoben, verarbeitet und/oder genutzt wurden (mindestens durch eine Protokollierung der Benutzerkennung des zugreifenden Mitarbeiters, des geänderten Datums und des Zeitpunktes der Änderung in den Logfiles der jeweiligen Systeme).

6 Auftragskontrolle

6.1 [ABC] sichert zu, das im jeweiligen Vertrag festgelegte Verfahren zur Authentifizierung beim Austausch von Kunden-Daten einzuhalten.

7 Verfügbarkeitskontrolle

7.1 [ABC] hat die Kunden-Daten durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung zu schützen. Vorsatz ist leider nicht einzuschränken.

7.2 [ABC] fertigt in regelmäßigen Abständen - mindestens einmal täglich - Sicherungskopien der Kunden-Daten an und sichert diese außerhalb der zur Leistungserbringung genutzten Räumlichkeiten. Die Wiederherstellbarkeit der gesicherten Daten ist stichprobenartig zu überprüfen und zu dokumentieren.

7.3 Soweit [ABC] Kunden-Daten auf selbst oder von Dritten betriebenen Servern erhebt, verarbeitet und/oder nutzt, ist dieser Server in einem separat abgesicherten Serverraum oder Rechenzentrum unterzubringen, welcher eine den Verfügbarkeitsanforderungen entsprechende Infrastruktur (mindestens aber USV, baulich brandschutzgerechte Ausführung, Brand- und Einbruchmeldeanlage und Klimatisierung) aufweist.

7.4 [ABC] verpflichtet sich, sämtliche Software auf Systemen, die zur Erhebung, Verarbeitung und Nutzung von Kunden-Daten eingesetzt werden, aktualisiert zu halten sowie sicherheitsrelevante Aktualisierungen (Updates, Patches, Fixes) unverzüglich einzuspielen, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht wurden und als unbedenklich eingestuft wurden.

8 Trennungsgebot

[ABC] verpflichtet sich, die Kunden-Daten so zu erheben, zu verarbeiten und/oder zu nutzen, dass eine vollständige Trennung der Kunden-Daten von Daten anderer Auftraggeber oder Eigendaten von [ABC] gemäß den vergebenen Zugriffsrechten gemäß Ziffer 3.1 (mindestens aber auf Ebene der zur Verarbeitung eingesetzten Anwendungen) gewährleistet ist. Insbesondere ist sicherzustellen, dass die Kunden-Daten jederzeit vollständig identifiziert und auch vollständig gelöscht werden können. Kunden-Daten, die zu unterschiedlichen Zwecken erhoben, verarbeitet und/oder genutzt werden, sind ebenfalls nach dieser Maßgabe getrennt voneinander zu erheben, zu verarbeiten und/oder zu nutzen.

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV
Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftragsdatenverarbeiter]

9 Löschen

9.1 Die Löschung betrifft nicht nur die erhobenen, verarbeiteten und/oder genutzten Kunden-Daten des Auftraggebers, sondern alle damit verbundenen Dateien und Daten in allen Systemen von [ABC] insbesondere auch in Sicherungs-, Archivierungs- und Telephoniesystemen.

9.2 [ABC] löscht sämtliche löschbaren elektronischen Datenträger, die Kunden-Daten enthalten, datenschutzgerecht und nicht wieder herstellbar. Ist aufgrund eines Defekts oder aufgrund der Eigenheiten des Datenträgers eine derartige Löschung nicht möglich, so ist der Datenträger entsprechend Ziffer 9.3 zu vernichten.

9.3 [ABC] vernichtet sämtliche Papierdokumente und alle nicht-löschbaren Datenträger, die Kunden-Daten enthalten, mit einem handelsüblichen Dokumentenvernichter gemäß der Sicherheitsstufe 3 oder einem mindestens gleichwertigen Verfahren. Defekte magnetische Datenträger, die nicht wie oben angegeben mechanisch vernichtet werden können (z.B. defekte Festplatten), sind mittels eines zugelassenen Datenträgervernichters zu entsorgen.

10 Verschlüsselung

[ABC] verpflichtet sich bei allen Übertragungen von Kunden-Daten diese Daten zu verschlüsseln