

An die Unternehmensleitung des Hyundai-Autohauses

Übermittlung von Servicedaten in Zusammenhang mit der HGSI Kundenzufriedenheitsstudie

Gemäß Vorgaben von Hyundai Motor Deutschland sollen Kunden soweit wie möglich per E-Mail zur HGSI-Kundenzufriedenheitsstudie eingeladen werden. Für E-Mail-Versendungen sowie ggfs. telefonische Kontaktaufnahmen gelten jedoch jeweils andere gesetzliche Regelungen hinsichtlich des Datenschutzes und der Zulässigkeit. Um Ihnen die Formalitäten möglichst zu erleichtern, stellen wir Ihnen einen Mustervertrag zur Verfügung, der den Anforderungen des Bundesdatenschutzgesetzes (BDSG) entspricht zusammen mit den geforderten technischen und organisatorischen Maßnahmen.

Für Sie bedeutet das konkret:

1. Bitte drucken Sie die beiliegenden Unterlagen aus und **senden** Sie den Vertrag paraphiert und **unterschrieben ausschließlich per Briefpost zurück** an die

aura Europa GmbH, Gartenstr. 3, 51379 Leverkusen
2. Die aura Europa GmbH wird den Vertrag ebenfalls unterzeichnen und Ihnen zur Aufbewahrung zurücksenden.
3. Solange der unterschriebene Vertrag nicht bei uns vorliegt, können wir die Kunden leider nicht per E-Mail anschreiben. Die Einladungen werden dann weiterhin postalisch versendet.
4. Unabhängig von den vertraglichen Gegebenheiten beachten Sie bitte, dass Sie nur dann die E-Mail-Adresse des Kunden für die HGSI-Kundenzufriedenheitsstudie hochladen dürfen, wenn dieser hierzu ausdrücklich und nachweislich gemäß der gesetzlichen Bestimmungen hinsichtlich der Verwendung seiner E-Mail-Adresse für Kundenzufriedenheitsumfragen **eingewilligt** hat.
5. Unabhängig von den vertraglichen Gegebenheiten beachten Sie bitte, dass Sie nur dann die Telefonnummer des Kunden für hochladen dürfen, wenn dieser hierzu ausdrücklich und nachweislich gemäß der gesetzlichen Bestimmungen hinsichtlich der Verwendung seiner Telefonnummer für den jeweiligen Zweck der Kontaktaufnahme **eingewilligt** hat.

Leverkusen, März 2015

aura Europa GmbH

Datenschutz- und Datensicherheitsbestimmungen

zwischen



– nachstehend Auftraggeber genannt –

und

aura Europa GmbH, Gartenstraße 3, 51379 Leverkusen

– nachstehend Auftragnehmer genannt –

Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsdatenverarbeitung i.S.d. § 11 Bundesdatenschutzgesetz (BDSG), die der Auftragnehmer gegenüber dem Auftraggeber erbringt.

§ 1 Gegenstand und Dauer des Auftrags

Der Auftragnehmer verarbeitet im Rahmen des Auftrags personenbezogene Daten des Auftraggebers für Zwecke der Hyundai HGS Kundenzufriedenheitsstudie.

Die Vereinbarung wird auf unbestimmte Zeit geschlossen.

Unabhängig von den vorstehenden Regelungen gelten die Verpflichtungen zum Datengeheimnis, die Geheimhaltungspflicht und vereinbarte Aufbewahrungsfristen über das Vertragsende hinaus.

§ 2 Umfang, Art und Zweck der Datenverarbeitung, die Datenarten und der Kreis der Betroffenen

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Es ist dem Auftragnehmer nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Die Verarbeitung und Nutzung der 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.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden.

Art der Daten

- Händler-Nummer
- Anrede
- Vorname
- Nachname
- Firma
- Anschrift (Straße, PLZ, Ort)
- Email (sofern Einwilligung vorliegt)
- Telefonnummer (sofern Einwilligung vorliegt)
- Handy-Nummer (sofern Einwilligung vorliegt)
- KFZ-Kennzeichen
- Datum der Erstzulassung
- Fahrgestell-Nummer
- Modell
- Servicedatum
- Art der Leistung

Kreis der Betroffenen

- Kunden des Auftraggebers
- Kontaktpersonen

§ 3 Technische und organisatorische Maßnahmen

Die als Anlage 1 beigefügte Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG (Datenschutz- und Datensicherheitskonzept) ist Teil dieser Vereinbarung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer diesen Antrag unverzüglich an den Auftraggeber weitergeben.

§ 5 Pflichten des Auftragnehmers gemäß § 11 Abs. 4 BDSG und vorzunehmende Kontrollen

Der Auftragnehmer wird zur Erfüllung des Vertrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einsetzen, die auf das Datengeheimnis nach § 5 BDSG verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht wurden.

Ferner ist der Auftragnehmer verpflichtet, die Vorschriften zur Bestellung des Datenschutzbeauftragten gemäß §§ 4f, 4g BDSG zu erfüllen.

Bestellter Beauftragte(r) für den Datenschutz ist:

Herr Daniel Schwaiger
BFS-Datenschutz GbR
Forsbachstraße 19
51145 Köln
02203 / 18 36 791 // daniel.schwaiger@bfs-datenschutz.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer ist verpflichtet, organisatorische und technische Maßnahmen nach § 9 BDSG in einem angemessenen Verhältnis zum angestrebten Schutzzweck umzusetzen. Dabei hat er durch geeignete Kontrollen sicherzustellen, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können, die übertragene Datenverarbeitung aufgabenbezogen getrennt von anderer Datenverarbeitung erfolgt und die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Er unterwirft sich eventuellen Kontrollmaßnahmen der Datenschutzaufsichtsbehörde und wird den Auftraggeber über eine eventuelle Kontrollmaßnahme unverzüglich informieren.

§ 6 Unterauftragsverhältnisse

Der Auftragnehmer kann zur Vertragserfüllung Dritte einsetzen.

Der Auftragnehmer wird alle mit diesem Vertrag übernommenen Verpflichtungen dem Subunternehmen selbstständig auferlegen. Der Unterauftrag ist schriftlich zu fixieren.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer durch Dritte als Nebenleistung zur Unterstützung bei der Vertragserfüllung in Anspruch nimmt (z.B. Telekommunikationsleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern). Der Auftragnehmer ist jedoch verpflichtet, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 7 Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer räumt dem Auftraggeber bezüglich der Einhaltung der Vorschriften über den Datenschutz und der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein jederzeitiges Besichtigungs- und Kontrollrecht, grundsätzlich nach vorheriger Ankündigung, ein. Der Auftragnehmer ist verpflichtet, im Fall von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen.

Unabhängig davon wird der Auftragnehmer den Nachweis der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG durch ein alle 36 Monate zu erneuerndes

Testat zum Beispiel von einer anerkannten Wirtschaftsprüfungsgesellschaft oder seinem betrieblichen Datenschutzbeauftragten nachkommen.

§ 8 Mitzuteilende Verstöße des Auftragnehmers

Bei begründetem Verdacht der Verletzung von in dieser Vereinbarung festgelegten Datenschutz- und Datensicherheitsbestimmungen durch den Auftragnehmer selbst, Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte wird der Auftragnehmer den Auftraggeber unverzüglich benachrichtigen. Das Gleiche gilt bei Verstößen gegen die allgemeinen Vorschriften zum Schutz personenbezogener Daten.

§ 9 Umfang der Weisungsbefugnisse

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail bestätigen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen das BDSG oder eine andere Vorschrift über den Datenschutz verstößt.

§ 10 Rückgabe überlassener Datenträger und Löschung

Der Auftragnehmer ist verpflichtet, die personenbezogenen Daten nach schriftlicher Weisung und im Übrigen bei Beendigung/Kündigung des Vertrags – nach den Vorgaben des Auftraggebers – vollständig datenschutzgerecht zu löschen oder an den Auftraggeber zurückzugeben soweit keine gesetzlichen oder vertraglichen Regelungen dem entgegenstehen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

§ 11 Sonstiges

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Für Nebenabreden ist die Schriftform erforderlich.

Leverkusen, den

, den

Auftragnehmer

Auftraggeber

Anlage:

technische und organisatorische Maßnahmen



aura Europa GmbH, Gartenstraße 3, 51379 Leverkusen

Technische und organisatorische Maßnahmen nach § 9 BDSG nebst Anlage zu § 9 BDSG

Inhaltsverzeichnis

Zutrittskontrolle (Nr. 1 der Anlage zu § 9 BDSG).....	2
Gebäude / Grundstück:	2
Zutrittsberechtigungen:.....	2
Schlüsselregelungen:	2
Zutrittskontrollierte Zonen:	2
Gebäudereinigung:	2
Zugangskontrolle (Nr. 2 der Anlage zu § 9 BDSG)	3
Zugang	3
Netzwerk	3
Passwörter.....	3
Zugangsberechtigungen	4
Internetprovider / verwendete Technik	4
Firewall	4
Browser	4
Systemadministration.....	4
Zugriffskontrolle (Nr. 3 der Anlage zu § 9 BDSG)	5
Allgemeiner Schutz	5
DV-Systeme	5
Passwörter.....	5
Netzwerk / Server.....	6
Fehlerdiagnose / Fernwartung	6
Notebooks / Smartphones.....	6
Papierhafte Unterlagen / Office-Dokumente	6
Data Loss Prevention	7
Datenträger / Datenträgerverwaltung	7
Weitergabekontrolle (Nr. 4 der Anlage zu § 9 BDSG).....	7
Arten der Übertragung	7
Protokollierung.....	7
Datensicherung	8
Mobile Datenträger.....	8
W-LAN	8
Fernwartung.....	8
Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG)	8
Berechtigungskonzept	8
Auftragskontrolle (Nr. 6 der Anlage zu § 9 BDSG)	9
Überprüfung des Auftragnehmers.....	9
Einbindung des DSB.....	9
Vertragsinhalte	9
Löschung von Restdaten.....	9
Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 BDSG)	10
Datensicherung	10
Virenschutz.....	10
Trennungsgebot (Nr. 8 der Anlage zu § 9 BDSG)	11
Datenbanken	11



Zutrittskontrolle (Nr. 1 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren)

Gebäude / Grundstück:

Die Büroräume befinden sich in der zweiten Etage eines Bürogebäudes mit insgesamt 4 Stockwerken und einem nutzbaren Keller und wird von unterschiedlichen Unternehmen genutzt. Das Gebäude liegt unmittelbar an der Straße und ist von außen gut beleuchtet. Der Haupteingang wird durch ein Sicherheitsschloss gesichert, Neben- und Hintereingänge sind zusätzlich noch mit einem Sperrriegel geschützt. Die verbauten Fenster bestehen aus Isolierverglasung. Lichtschächte, Lüftungsöffnungen, Feuerleiter oder Feuertreppe über die sich ein Unbefugter eventuell Zutritt verschaffen könnte, existieren nicht.

Zutrittsberechtigungen:

Besucher müssen sich zwangsläufig am Empfang melden und werden in den Büroräumlichkeiten begleitet. Die Bearbeitungszonen sind von den Publikumszonen getrennt. Vor Feierabend werden die Räumlichkeiten überprüft, um zu verhindern, dass sich Unbefugte einschließen lassen.

Schlüsselregelungen:

Sämtliche Schlüssel sind in einem Schlüsselregister aufgeführt, sowohl die Schlüsselausgabe wie auch die Schlüsselnahme werden quittiert. Überzählige Schlüssel sind in ausreichend sicher gestalteten Schlüsselkästen deponiert.

Die Schlüssel der Mitarbeiter sind der Art, dass sie nicht einfach unbefugt dupliziert werden können. Sollte ein Mitarbeiter seinen Schlüssel verlieren oder ein ausgeschiedener Mitarbeiter seinen Schlüssel nicht zurückgeben, so werden unverzüglich die Schlösser ausgetauscht.

Der Generalschlüssel befindet sich bei der Geschäftsführung.

Zutrittskontrollierte Zonen:

Alle Datenverarbeitungsanlagen mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, befinden sich in zugriffskontrollierten Zonen. Die Zutrittskontrollmaßnahmen sind den Mitarbeitern bekannt gemacht worden und werden beachtet.

Alle Server / Firewalls sind in einem abgeschlossenen Raum („Serverraum“) installiert. Dadurch ist auch sichergestellt, dass zum Serverraum nur befugte Personen Zutritt haben. Zusätzlich sind die Server noch in einem speziellen Serverschrank verschlossen.

Büros und Büroschränke werden mit verschiedenen Schlüsseln verschlossen. So wird verhindert, dass Mitarbeiter unbefugt Schränke öffnen können und somit Zugriff auf personenbezogene Daten erhalten, die nicht zu ihrem Aufgabengebiet gehören.

Aufbewahrungsorte für mobile Endgeräte sind bei den Zutrittskontrollmaßnahmen berücksichtigt.

Gebäudereinigung:

Die Gebäudereinigung findet innerhalb der Geschäftszeiten statt. In datenschutzrechtlichen Räumlichkeiten arbeiten die Reinigungskräfte stets unter Aufsicht. Die Reinigungskräfte besitzen



keinerlei Gebäudeschlüssel und müssen sich somit bei Betreten der Büroräumlichkeiten der aura Europa GmbH am Empfang melden.

Zugangskontrolle (Nr. 2 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)

Zugang:

Die Server werden durch ein abgeschlossenes Serrack gegen unbefugten Zugang gesichert und mittels Bootschutz gegen unbefugte Benutzung geschützt.

Netzwerk:

Es besteht die Möglichkeit der Softwareverriegelung der Bildschirme, diese wird auch genutzt. Die Weiterarbeit ist dann erst nach Eingabe eines Passwortes möglich. Zudem aktiviert sich die Bildschirmsperre nach 10 Minuten Inaktivität automatisch. Weiterhin sind die Mitarbeiter angewiesen, die Endgeräte und/oder Personal Computer beim Verlassen des Arbeitsplatzes gegen unbefugte Benutzung zu sperren und diese nach Beendigung der Arbeit herunterzufahren.

Die Abschottung des internen Netzes gegen ungewollte Zugänge von außen erfolgt mittels einer Firewall. Sämtliche Anmeldeversuche ans Netzwerk werden protokolliert und können bei Bedarf kontrolliert und ausgewertet werden. Bei mehrmaliger fehlerhafter Anmeldung wird als Sanktion die Benutzerberechtigung gesperrt. Diese Sperre kann nur von einem Administrator aufgehoben werden.

Jeder DV-Benutzer verfügt über einen eigenen individuellen Benutzercode („User-ID“) zuzüglich eines selbstgewählten Passworts ohne welche eine Anmeldung am System nicht möglich ist. Da der Schutzbedarf bei den nur der Geschäftsführung zugänglichen Daten höher bewertet wird, erfolgt hier eine zusätzliche biometrische Identifizierung und Authentifizierung mittels Fingerprintreader.

Passwörter:

Die Regeln für Anforderungen an sichere Passwörter sind schriftlich in einer Richtlinie dokumentiert und werden durch eine Systemeinstellung erzwungen. Das jeweilige Passwort muss eine Mindestlänge von 7 Zeichen haben. Zudem müssen Groß- und Kleinbuchstaben sowie Ziffern enthalten sein. Es werden keine Gruppenpasswörter sondern ausschließlich Individualpasswörter vergeben. Das vom Administrator für den jeweiligen Benutzer voreingestellte Passwort muss der Benutzer bei seiner ersten Anmeldung ändern.

Bei der aura Europa GmbH wird das „Single sign on“-Verfahren genutzt. Dies bedeutet, dass der Benutzer mittels einmaliger Authentifizierung (Benutzername und Passwort) am Arbeitsplatz Zugriff auf alle Rechner und Dienste erhält, für die er lokal berechtigt ist.

Bei Pausen oder einer Abwesenheit von mehr als 10 Minuten aktiviert sich die Bildschirmsperre mit Passwortschutz automatisch und kann nur mittels Passworteingabe wieder aufgehoben werden. Nach 3 Fehlversuchen bei der Eingabe wird das Benutzerkonto gesperrt.



Die Übertragung der Passwörter im Netz erfolgt verschlüsselt nach dem Stand der Technik (AES-256). Darüber hinaus werden die Passwörter verschlüsselt abgespeichert, so dass ein Zugriff unbefugter Personen darauf ausgeschlossen ist.

Die Default-Passwörter aller Systeme wurden deaktiviert beziehungsweise geändert. Für das Bios existiert ein separates Passwort. Das Administrationspasswort ist ausschließlich der Geschäftsführung bekannt.

Zugangsberechtigungen:

Die maschinelle Verwaltung und Pflege der Zugangsberechtigungen ist eindeutig geregelt, Zugangsberechtigungen von ausgeschiedenen Mitarbeitern werden sofort gelöscht. Bei als missbräuchlich erkannten Zugangsversuchen werden Sanktionen wie beispielsweise die Sperrung des betroffenen Benutzerkontos getroffen.

Sich „unterwegs“ befindliche Datenträger werden / sind stets nach dem Stand der Technik verschlüsselt (AES-256).

Sensible Papierunterlagen werden im Büro der Geschäftsführung in einem Büroschrank aufbewahrt. Besonders sensible Unterlagen befinden sich in einem verschlossenen Tresor im Büro der Geschäftsführung. Dieses Büro ist bei Abwesenheit verschlossen.

Internetprovider / verwendete Technik:

Es wird ein sogenanntes „Corporate Network“ genutzt. Hierbei werden räumlich verteilte Einzelnetze der Muttergesellschaft, aura Corporation UK Limited, mit denen der aura Europa GmbH mittels eines externen Providers vernetzt. Es wird streng darauf geachtet, dass die Muttergesellschaft nur auf die Daten Zugriff hat, die dafür freigegeben sind. Zur Sicherstellung dessen wird ein separates physikalisches Laufwerk mit den Daten zur Verfügung gestellt. Als technische Verbindungskomponente zur Einwahl wird ein DSL-Router eingesetzt.

Firewall:

Als weiteres Zugangskontrollmedium wird eine Softwarefirewall eingesetzt, die automatisch laufend neu erschienene Updates installiert. Darüber hinaus wird ein Proxy-Server als Netzwerkkomponente genutzt.

Browser:

Es wird ausschließlich der Internet Explorer von Microsoft eingesetzt. Sicherheitsupdates und Patches werden in einem automatisierten Verfahren laufend bei Erscheinen installiert.

Die Sicherheitseinstellungen werden zudem regelmäßig durch Penetrationstests (Prüfung der Sicherheit mit Mitteln und Methoden die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen) überprüft.

Systemadministration:

Die Systemadministration erfolgt anhand einer Administrationsrichtlinie. Die Administrationsarbeit teilt sich die Geschäftsführung der aura Europa GmbH mit einem externen Dienstleister, der COMPUMASTER GmbH, Rhein-Mosel-Straße 14, 56281 Emmelshausen. Allerdings kann sich der



Datenschutz GbR



Dienstleister nur mit technischer Freigabe durch die aura Europa GmbH auf die DV-Systeme aufschalten und die Arbeiten werden dann stets im 4-Augen-Prinzip durchgeführt.

Abweichend von den Nutzerpasswörtern existieren spezielle Passwortkonventionen zu den Administrationspasswörtern.

Zugriffskontrolle (Nr. 3 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, 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)

Allgemeiner Schutz:

Sensible Daten sind gegen (zufällige) Kenntnisnahme durch Unbefugte durch blickdichte Türen geschützt.

Das Unternehmen schützt sich gegen Malware und unbefugte Zugriffe durch eine Antivirensoftware mit täglichen automatisierten Updates.

Es werden Verschlüsselungsverfahren nach dem Stand der Technik (AES-256) eingesetzt.

DV-Systeme:

Für die Benutzung der DV-Systeme mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, müssen Benutzerkennungen nebst Passwort eingegeben werden. Hierzu existieren sowohl Regelungen, wer die Benutzerkennungen einrichtet, als auch Richtlinien für die Vergabe der Benutzerkennungen als solche. Grundsätzlich erfolgt die Berechtigung jeweils auf standardisiertem Wege (und nicht auf Zuruf) und nach dem 4-Augen-Prinzip. Die erteilten Berechtigungen werden stichprobeartig überprüft. Dadurch ist gewährleistet, dass jeder Benutzer nur auf diejenigen Dienste zugreifen kann, die er zur Erfüllung seiner Aufgaben benötigt.

Das System ergreift von sich aus Sanktionen bei mehrfach missbräuchlichen Zugriffsversuchen in Form einer Benutzersperre die ausschließlich von einem Administrator aufgehoben werden kann.

Darüber hinaus unterstützen die DV-Systeme eine Zugriffssicherung durch verstecken, schreibschützen, verschlüsseln und sperren von Dateien und Verzeichnissen.

Eine Beschränkung der Anmeldezeiten ist möglich.

Passwörter:

Die Regeln für Anforderungen an sichere Passwörter sind schriftlich dokumentiert. Das jeweilige Passwort muss eine Mindestlänge von 7 Zeichen haben. Zudem müssen Groß- und Kleinbuchstaben

sowie Ziffern enthalten sein. Es werden keine Gruppenpasswörter sondern ausschließlich Individualpasswörter vergeben. Das vom Administrator für den jeweiligen Benutzer voreingestellte Passwort muss der Benutzer bei seiner ersten Anmeldung ändern.

Bei der aura Europa GmbH wird das „Single sign on“-Verfahren genutzt. Dies bedeutet, dass der Benutzer mittels einmaliger Authentifizierung (Benutzername und Passwort) am Arbeitsplatz Zugriff auf alle Rechner und Dienste erhält, für die er lokal berechtigt ist.



Bei Pausen oder einer Abwesenheit von mehr als 10 Minuten aktiviert sich die Bildschirmsperre mit Passwortschutz automatisch und kann nur mittels Passworteingabe wieder aufgehoben werden. Nach 3 Fehlversuchen bei der Eingabe wird das Benutzerkonto gesperrt.

Die Übertragung der Passwörter im Netz erfolgt verschlüsselt nach dem Stand der Technik (AES-256). Darüber hinaus werden die Passwörter verschlüsselt abgespeichert, so dass ein Zugriff unbefugter Personen darauf ausgeschlossen ist.

Die Default-Passwörter aller Systeme wurden deaktiviert beziehungsweise geändert. Für das Bios existiert ein separates Passwort. Das Administrationspasswort ist ausschließlich der Geschäftsführung bekannt.

Netzwerk / Server:

Für den Zugriff auf das Netzwerk ist die Eingabe einer Benutzerkennung und eines Passwortes notwendig. Die Rechtevergabe erfolgt benutzerspezifisch abgestuft auf Verzeichnis- und Dateiebene und ist an ein Endgerät beziehungsweise an eine Gruppe von Endgeräten gebunden.

Die Betriebssystemebene ist für den normalen Anwender grundsätzlich gesperrt.

Um unberechtigte Dateizugriffe feststellen zu können, werden Protokolle geführt und diese regelmäßig ausgewertet.

Fehlerdiagnose / Fernwartung:

Es wurden Sicherheitsmaßnahmen für die Fehlerdiagnose, Wartung und Fernwartung ergriffen, so dass anhand von Protokollen erkennbar ist, wer wann worauf zugegriffen hat. Diese Protokolle werden regelmäßig ausgewertet.

Der Zugriff per Fernwartung erfolgt ausschließlich durch betriebliche Computer, die über mindestens den gleichen Sicherheitsstandard verfügen wie die lokalen PCs.

Notebooks / Smartphones:

Es existiert eine Richtlinie für den Umgang mit mobilen Endgeräten. Darüber hinaus werden die mobilen Endgeräte außerhalb der Geschäftszeiten sicher verschlossen aufbewahrt.

Papierhafte Unterlagen / Office-Dokumente:

Der Zugriff auf papierhafte Unterlagen wird geschützt:

Papierunterlagen / Akten werden sicher verschlossen, zu vernichtende Papierunterlagen / Akten werden unverzüglich durch den Mitarbeiter mittels eines Shredders (Sicherheitsstufe 4) vernichtet.

Sensible Daten werden unmittelbar auf lokalen Druckern gedruckt, so dass sichergestellt ist, dass unbefugte Dritte diese Ausdrücke nicht einsehen können.

Somit haben unbefugte Dritte, wie etwa auch das Reinigungsunternehmen, keinen Zugriff auf papierhafte Unterlagen.

Office-Dokumente werden durch Konvertierung ins pdf-Format vor Manipulation geschützt.



Data Loss Prevention:

Bei der aura Europa GmbH wird „Data Loss Prevention“ (Schutz gegen unerwünschten Abfluss von Daten, der Schaden verursacht und auch bemerkt wird) beachtet:

Sensible Daten werden verschlüsselt und können nur von befugten Mitarbeitern eingesehen werden, das Speichern von sensiblen Daten auf mobilen Datenträgern sowie der Versand von sensiblen Daten erfordern spezielle Berechtigungen.

Die externen Administratoren können die Daten in der Regel somit nicht einsehen.

Datenträger / Datenträgerverwaltung:

Verantwortlich für die Datenträger ist die Geschäftsführung.

Die genutzten beweglichen Datenträger sind in einer Auflistung erfasst und die Aktualität wird durch regelmäßige Datenträgerinventuren sichergestellt. Darüber hinaus werden eigene Datenträger besonders gekennzeichnet, so dass sie einfach von fremden Datenträgern unterschieden werden können, auch erhält jeder Kunde seinen „eigenen“ Datenträgerpool.

Die verwendeten Datenträger werden mittels Fingerprint der Geschäftsführung ver beziehungsweise entschlüsselt. Die Verschlüsselung entspricht dem Stand der Technik (AES-256). Zugriffssicher aufbewahrt werden die Datenträger im Büro der Geschäftsführung.

Nicht mehr benötigte und defekte Datenträger werden durch physische Zerstörung unbrauchbar gemacht und sodann datenschutzgerecht entsorgt. Die ordnungsgemäße Vernichtung wird kontrolliert. Sofern Datenträger erneut verwendet werden sollen oder deren Weitergabe geplant ist, erfolgt vorher eine datenschutzgerechte Löschung.

Weitergabekontrolle (Nr. 4 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, 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)

Arten der Übertragung:

Der Versand von Daten erfolgt per E-Mail, sFTP und HTTPs, zur Übertragung wird das Internet genutzt. Die Berechtigten identifizieren sich mittels Benutzerkennung und Passwort.

Voice over IP (VoIP) wird nicht genutzt.

Sofern öffentliche Netzwerke wie beispielsweise WLAN-Hotspots außerhalb der Büroräume genutzt werden, wird die Firewall der mobilen Computer auf „öffentliches Netzwerk“ umgestellt damit Netzwerkfreigaben von außen nicht mehr erreichbar sind.

Protokollierung:

Es hat eine genaue Festlegung der Übermittlungswege und Datenempfänger stattgefunden, die Datenübermittlungsaktivitäten werden protokolliert. Vorgesehene Datenübermittlungen werden in den Verfahrensübersichten erfasst.



Datensicherung:

Daten werden vor dem Transport verschlüsselt und auch verschlüsselt übertragen. Malwarebedingter Manipulation wird durch Verschlüsselung und dem Einsatz eines Virenschanners vorgebeugt.

Bei Bedarf können E-Mails mit einer elektronischen Signatur versehen werden, so dass der Empfänger sicher beurteilen kann, ob die E-Mail vom angeblichen Absender stammt.

Es werden keine E-Mail Server eingesetzt, die unverschlüsselt über das Internet erreichbar sind damit ausgeschlossen ist, dass Passwörter für SMTP und POP3 abgehört werden können.

Mobile Datenträger:

Bei den eingesetzten Notebooks sind einzelne Partitionen beziehungsweise Verzeichnisse verschlüsselt.

Es werden ausschließlich USB-Sticks und externe Festplatten mit festeingebauter Verschlüsselung verwendet.

W-LAN:

Es gibt betriebsinterne W-LAN-Zugänge, diese werden per WPA(2) abgesichert.

Fernwartung:

Fernwartung wird durchgeführt für die Wartung von Hardware, Software und zur Benutzeradministration / Helpdesk. Um sich durch das Internet aufschalten zu können ist ein explizites Freischalten durch den Auftraggeber notwendig. Der Übertragungsweg ist hierbei verschlüsselt. Es erfolgt eine Zugangskontrolle durch die notwendige Eingabe von Benutzerkennung und Passwort. Für die Dauer der Fernwartung werden Administrationsrechte gewährt, diese werden zudem durch Monitoring überwacht.

Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

Berechtigungskonzept:

Ein Berechtigungskonzept regelt die Eingabe, Veränderung und Löschung von Daten.

Sämtliche Konfigurationsänderungen aktiver Netzwerkkomponenten werden protokolliert.

Dateizugriffe und auch Dateilöschungen werden in den Security Logs protokolliert, die Protokolldateien nach 14 Tagen überschrieben.



BFS-Datenschutz GbR



Auftragskontrolle (Nr. 6 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

Überprüfung des Auftragnehmers:

Der Auftragnehmer wird sorgfältig anhand von festgelegten Kriterien wie Referenzen und Zertifizierungen / Gütesiegel durch die Geschäftsführung der aura Europa GmbH ausgewählt. Bei der Auswahl des Auftragnehmers wird sichergestellt, dass dieser geeignet ist, die gestellten Aufgaben ordnungsgemäß zu erledigen. Es finden von Beginn und dann regelmäßig Überprüfungen des Auftragnehmers statt, ob dieser die vertraglichen Regelungen einhalten kann und einhält und ob er darüber hinaus in jedem Fall nachweisen kann, dass ausreichende und geeignete Datensicherungsmaßnahmen getroffen wurden. Diese Überprüfungen werden schriftlich dokumentiert.

Die Auftraggeberin hat in diesem Zusammenhang Kenntnis von der Verpflichtungserklärung auf § 5 BDSG der Mitarbeiter des Auftragnehmers.

Die aura Europa GmbH ist auch selber als Auftragnehmerin tätig.

Einbindung des DSB:

Der Datenschutzbeauftragte ist bei allen Verträgen sowie bei der Prüfung der ordnungsgemäßen Durchführung der Auftragsdatenverarbeitung einbezogen und verfügt über eine Übersicht sämtlicher Fälle. Aus dieser Dokumentation sind die personellen Zuständigkeiten bei der verantwortlichen Stelle ersichtlich.

Vertragsinhalte:

Es wird bei jedem Auftrag geprüft, welche rechtlichen Maßnahmen die Auftragsvergabe abstützen, jede Auftragsdatenverarbeitungsvereinbarung wird stets schriftlich abgeschlossen. Hierbei sind die zu erfüllenden technischen und organisatorischen Maßnahmen des Auftragnehmers Bestandteil der Vereinbarung. Auch sind die Kompetenzen und Pflichten zwischen Auftraggeberin und Auftragnehmer klar abgegrenzt, insbesondere ist in diesem Zusammenhang sichergestellt, dass sich die Auftraggeberin eindeutig identifizieren muss und ihre Beauftragten befugt sind, dem Auftragnehmer Weisungen zu erteilen.

Es existieren detaillierte Regelungen der Auftragsverhältnisse und Formalisierungen des gesamten Auftragsablaufs, auch zum Einsatz von Subunternehmen sowie eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Transport von Datenträgern) bezüglich der Datenerhebung, Datenerfassung und Datenverarbeitung.

Es wird in der Vereinbarung ebenfalls vorgeschrieben, wie der Auftragnehmer nicht mehr benötigte Unterlagen zu behandeln hat.

Löschung von Restdaten:

Bei der Aushändigung maschinell lesbarer Datenträger ist sichergestellt, dass sich darauf keine Restdaten, etwa von anderen Verarbeitungen, befinden.



Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind)

Datensicherung:

Die Verantwortlichkeiten für die zentrale Datensicherung sind geregelt, Zugriff auf die Sicherungsdatenträger hat lediglich die Geschäftsführung. Sicherungsdatenträger sind zusätzlich ausgelagert.

Es erfolgt täglich eine automatisch erzwungene Sicherung in Form eines Vollbackups. Hierbei werden sowohl der Datenstatus wie auch der Systemstatus gesichert. Zusätzlich kann „auf Knopfdruck“ ebenfalls ein Vollbackup des Datenstatus durchgeführt werden. Die Backups werden verschlüsselt aufbewahrt und zusätzlich auf einer NAS gespiegelt.

Die Lesbarkeit der Sicherungen wird täglich per Systemtest überprüft.

Es ist festgestellt worden, wie lange im Notfall auf das Netzwerk verzichtet werden könnte. Mit der Aufnahme eines Notbetriebs (zum Beispiel beim Ausfall eines Servers) kann innerhalb eines vertretbaren Zeitraums begonnen werden.

Die zentrale und einheitliche Beschaffung von Hard- und Software ist geregelt.

Virenschutz:

Es werden Virenschutzprogramme eingesetzt. Diese erkennen sowohl unbekannte Schadsoftware mittels heuristischer Verfahren als auch Schadsoftware in verschlüsselten Dateien. Die Updates der Virenschutzprogramme erfolgen automatisiert täglich. Als zusätzliche Schutzmaßnahme werden SPAM-Filter genutzt.

Schutz der PC-Arbeitsräume und Server vor Feuer, Wasser und Überspannung/Stromausfall

In den Büroräumen sowie im separaten Serverraum herrscht striktes Rauchverbot. Sollte dennoch in den PC-Arbeitsräumen oder im Serverraum ein Feuer ausbrechen, so stehen Feuerlöscher bereit.

Es verlaufen keine Wasserrohre direkt über den Computerkomponenten. Die Serverkomponenten und Leitungen werden zusätzlich vor Wasser dadurch geschützt, dass sie sich mindestens 20cm über dem Fußboden befinden.

Eine Unterbrechungsfreie Stromversorgung (USV) sichert die PC-Arbeitsplätze, die Server, die zentralen Netzwerkkomponenten sowie die Telefonanlage gegen einen unerwarteten Stromausfall ab und schützt zusätzlich vor Überspannungen. Die USV wird regelmäßig gewartet und getestet.



Datenschutz GbR



Trennungsgebot (Nr. 8 der Anlage zu § 9 BDSG)

(es sind Maßnahmen zu treffen die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)

Datenbanken:

Es sind logische Datenbanken eingerichtet, Datenbankabfragen sind mit besonderen Privilegien geschützt. Die Benutzer werden in der Verwendung der Datenbanken geschult.

Daten verschiedener Kunden werden stets in eigenen Verzeichnissen gespeichert, so dass Löschfristen individuell entsprochen werden kann.

Zugriffe über Anwendungen werden ausschließlich nach Erfordernis eingerichtet.

Es gibt klare Regelungen für die Archivierung.

Die technischen und organisatorischen Maßnahmen wurden in Zusammenarbeit mit dem externen Datenschutzbeauftragten – Herrn Daniel Schwaiger, BFS-Datenschutz GbR, daniel.schwaiger@bfs-datenschutz.de, +49 (0)2203 / 18 36 791 – aufgenommen und geprüft.

Auf die konkrete Benennung von einzelnen Komponenten wurde aus Sicherheitsgründen bewusst verzichtet. Nichtsdestotrotz wurden diese erfasst und sind separat dokumentiert.

BFS-Datenschutz GbR | August 2013

aura Europa GmbH | August 2013