Cord Media Digital Services
Frank Oschatz
Schwarze-Breite-Str. 11
73760 Ostfildern

Telefon:+49 173 / 89 20 755
Telefax: +49 711 / 90 004 153

info@cordmedia.de
www.cordmedia.de

BW-Bank
BLZ 60050101 • Konto 66 80 462
IBAN DE 53 60050101 0006680462
BIC SOLADEST600
Umsatzsteuer-ID: DE244043427
Steuer Nr. : 59300 / 46410
Betriebsnummer: 93130109

Vertrag zur Auftragsverarbeitung mit Vereinbarung zum Datenschutz

gemäß Art. 28 DS-GVO

Anlage B „Technisch organisatorisch Maßnahmen“

Cord Media Digital Services
Frank Oschatz
Schwarze-Breite-Str. 11
73760 Ostfildern

Telefon:+49 173 / 89 20 755
Telefax: +49 711 / 90 004 153
info@cordmedia.de
www.cordmedia.de

BW-Bank
BLZ 60050101 • Konto 66 80 462 IBAN DE
53 60050101 0006680462
BIC SOLADEST600

Umsatzsteuer-ID: DE244043427
Steuer Nr. : 59300 / 46410
Betriebsnummer: 93130109

Inhalt

Cord Media Digital Services
Frank Oschatz
Schwarze-Breite-Str. 11
73760 Ostfildern

Telefon:+49 173 / 89 20 755
Telefax: +49 711 / 90 004 153
info@cordmedia.de
www.cordmedia.de

BW-Bank
BLZ 60050101 • Konto 66 80 462
IBAN DE 53 60050101 0006680462
BIC SOLADEST600

Umsatzsteuer-ID: DE244043427
Steuer Nr. : 59300 / 46410
Betriebsnummer: 93130109

Dies ist die Anlage B zur Datenschutzvereinbarung zur Verarbeitung personenbezogener Daten im Auftrag mit Cord Media. Folgende Ausführungen informieren Sie als Kunden über die Maßnahmen, die Cord Media zum Schutz personenbezogener Daten getroffen hat. Dieser Maßnahmenkatalog wird jährlich geprüft und aktualisiert. Eine Versionierung wird lediglich intern dokumentiert. An dieser Stelle finden Sie die stets die aktuelle Version des Maßnahmenkataloges. Wir haben diese Darstellung gewählt, um den Umfang des AV-Vertrages in einem vertretbaren Umfang zu halten und die Umwelt zu schonen! Es steht Ihnen frei sich diese Seiten auszudrucken oder als PDF-Dokument zu speichern.

Vertraulichkeit

Zutrittskontrolle

Mit der Zutrittskontrolle soll unbefugten die räumliche Annährung an Datenverarbeitungsanlagen verwehrt werden! Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

Protokollierung von Besuchern und Dienstleistern: Besucher und Dienstleister, erhalten nur nach vorheriger Anmeldung Zugang zu den Büroräumen. Zudem werden Besucher und Dienstleister namentlich erfasst und deren Besuchszeiten protokolliert.

Verwendung sicherer Türen und Fenster: Innerhalb des gesamten Bürogebäudes sind moderne und einbruchsichere Türen und Fenster der Widerstandsklasse RC2 verbaut. Die Fenster sind zusätzlich mit einem Sichtschutz versehen, um einen direkten Einblick in die Büroräume zu verhindern.

Zugangskontrolle

Mit der Zugangskontrolle soll verhindert werden, dass unbefugte Zugang zu IT-Systemen erhalten. Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT- Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Automatisches Sperren von PCs / Macs nach fünf Minuten: Alle im Einsatz befindlichen Arbeitsplatzrechner (PCs, Macs) rufen nach fünfminütiger Inaktivität automatis ch die Anmeldemaske des jeweiligen Betriebssystems auf. Ein Zugriff auf die Arbeitsplatzrechner ist dann nur nach vorheriger Eingabe des Nutzerpassworts möglich. So wird verhindert, dass Unbefugte beispielsweise während der Pausenzeiten Zugriff auf kritische Daten erlangen können.

Tägliches Aufräumen der Arbeitsplätze (“Clean desk”): Die Schreibtische im gesamten Bürogebäude werden stets vor dem Feierabend bzw. dem Wochenende aufgeräumt. In dies em Zuge werden vertrauenswürdige Dokumente mit personenbezogenen Daten sicher verwahrt (z. B. durch das Verschließen in einem Schrank). So kann verhindert werden, dass Dokumente mit personenbezogenen Daten versehentlich entsorgt werden (z. B. durch Reinigungskräfte) oder unberechtigte Personen Zugang zu diesen Dokumenten erlangen.

Verwendung einer Firewall: Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Verwendung personalisierter Logins: Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktio-

nen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.

Verwendung sicherer und individueller Passwörter: Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sicher gestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nach wie vor gewahrt.

Verwendung und regelmäßige Aktualisierung eines Virenscanners: Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch aus gewählte Mitarbeiter möglich.

Zugriffskontrolle

Unter Zugriffskontrolle versteht man, dass nur berechtigte Benutzer Daten in IT-Systemen erheben, verarbeiten und nutzen dürfen. Es ist sicherzustellen, 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 oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation eingerichteter Zugänge für Mitarbeiter: Alle Zugänge zu internen und externen Systemen werden vor deren Einrichtung dokumentiert. Dabei werden der Name des Mitarbeiters, das jeweilige System sowie der eingerichtete Benutzername protokolliert. Diese Informationen stellen die Basis dafür dar, dass bei einem späteren Austritt zielgerichtet die Zugänge des jeweiligen Mitarbeiters gesperrt bzw. gelöscht werden können.

Minimale Anzahl an Mitarbeitern mit administrativen Rechten: Um zu gewährleisten, dass lediglich autorisierte Personen Zugriff auf kritische IT-Systeme sowie darauf gespeicherter Daten haben, verfügen nur aus gewählte Mitarbeiter über die notwendigen administrativen Rechte. Diese Mitarbeiter schalten projektbezogen die Zugriffsrechte der anderen Mitarbeiter frei, sofern diese für ihre Arbeit notwendig sind. Nach Abschluss der jeweiligen Arbeiten werden die entsprechenden Rechte wieder entzogen. So wird die Anzahl der Mitarbeiter, die theoretisch Zugriff auf alle im Unternehmen gespeicherten personenbezogenen Daten haben, auf ein absolutes Minimum reduziert.

Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme: Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die diesen eigentlich nicht gestattet wären.

Sicheres Löschen von Daten auf Datenträgern: Werden Daten mit personenbezogenem Inhalt auf lokalen Datenträgern gelöscht, erfolgt dies grundsätzlich durch Anwendung spezieller Löschprogramme. So werden auch vom Betriebssystem angelegte Schattenkopie sowie Daten auf SSD-Speichermedien zuverlässig gelöscht. Eine nachträgliche Wiederherstellung der gelöschten Daten ist so nicht mehr möglich.

Sperrung von Zugängen beim Austritt von Mitarbeitern: Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für

interne und externe Systeme. Als Basis für diesen Vorgang wird die Dokumentation der zuvor angelegten Zugänge verwendet. In der Dokumentation wird abschließend ebenfalls die Sperrung bzw. Löschung der Zugänge vermerkt.

Verwendung sicherer und individueller Passwörter: Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sicher gestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nach wie vor gewahrt.

Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

Beauftragung zuverlässiger Transportunternehmen: Beim Versand von Daten auf dem Postweg oder beim Transport von Servern wird darauf geachtet, dass nur zuverlässige und vertrauenswürdige Transportunternehmen eingesetzt werden.

Sorgfältige Auswahl von Transportunternehmen und -fahrzeugen: Beim physischen Transport von personenbezogenen Daten (z. B. Übermittlung großer Datenmengen auf einer Blu-ray Disc durch einen Kurier) werden nur aus gesuchte und zuverlässige Transportunternehmen mit einwandfreier Reputation beauftragt, die zudem über die notwendige Erfahrung für einen Transport von sensiblen Daten verfügen. Auch die Verfügbarkeit geeigneter Transportfahrzeuge hat Einfluss auf die Auswahl. Nach erfolgreicher Übermittlung wird zudem die Rückmeldung des Empfängers eingeholt, welcher ebenfalls zu seiner Erfahrung mit dem Transportunternehmen befragt wird.

Nutzung SSL-verschlüsselter Übertragungswege im Internet: Für die Übermittlung von Daten mit personenbezogenem Inhalt über das Internet werden ausschließlich SSL/TLS -verschlüsselte Übertragungswege genutzt. Die gesicherte Verbindung zwischen Browser und Zielserver stellt sicher, dass Daten zwischen diesen beiden Systemen nicht von Dritten eingesehen oder manipuliert werden können.

Sicheres Löschen von Daten auf Datenträgern: Werden Daten mit personenbezogenem Inhalt auf lokalen Datenträgern gelöscht, erfolgt dies grundsätzlich durch Anwendung spezieller Löschprogramme. So werden auch vom Betriebssystem angelegte Schattenkopie sowie Daten auf SSD-Speichermedien zuverlässig gelöscht. Eine nachträgliche Wiederherstellung der gelöschten Daten ist so nicht mehr möglich.

Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Es soll eine getrennte Verarbeitung sichergestellt werden, damit keine Zweckentfremdung der personenbezogenen Daten möglich ist. Der Zweck für den die Daten erhoben wurden, darf nicht geändert werden. Aus diesem Grund ist es wichtig, dass Daten, die zu unterschiedliche Zwecken erhoben wurden, vollständig getrennt voneinander gespeichert werden. (Zweckbindungsgrundsatz)

Beim Auftragnehmer umgesetzte Maßnahmen:

Trennung von Live- und Entwicklungssystemen: Für die Entwicklung und Programmierung stehen den Entwicklern eigene Entwicklungsumgebungen mit anonymisierten oder pseudonymisierten Testdaten zur Verfügung, sodass eine Entwicklung am Produktivsystem mit den darin gespeicherten

Echtdaten nicht notwendig ist. So kann verhindert werden, dass versehentlich eine ungewollte Veränderung oder Weitergabe von personenbezogenen Daten erfolgt. Ausschließlich die gemeinsam mit dem Endkunden durchgeführten Live-Tests vor Projektabschluss erfolgen unter Zuhilfenahme der jeweiligen Echtdaten.

Verwendung von Zugriffsberechtigungen für interne Systeme: Alle internen Systeme sind vor unbefugtem Zugriff gesichert. Es ist nicht möglich, diese ohne eine weitere Anmeldung zu verwenden, wenn man sich im Firmennetzwerk befindet. Die Berechtigungen zur Nutzung der verschiedenen Systeme werden individuell vergeben und können individuell und systembezogen widerrufen werden. Ein genereller Zugriff auf alle im Firmennetzwerk befindlichen Daten wird somit unterbunden.

Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beim Auftragnehmer umgesetzte Maßnahmen:
Verwendung von pseudonymisierten Daten im Arbeitsalltag: Maßnahmen zur Pseudonymisierung von Daten erfolgen aktuell nicht.

Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:
Verwendung verschlüsselter Übertragungswege für den Datenaustausch: Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten könnten, findet dies ausschließlich auf sicheren und verschlüsselten Übertragungswegen statt. Es werden ins besondere SSH-Verbindungen genutzt und keine unverschlüsselten Protokolle verwendet, wenn verschlüsselte Alternativen zur Verfügung stehen. So werden E-Mails zum Beispiel via IMAP nur mit SSL/TLS oder HTTPS -Verbindungen abgerufen und versendet.

Verwendung von SSL-Zertifikaten für Hostingumgebungen: Alle von uns betreuten Webseiten sowie die hierfür genutzten Hosting-Umgebungen, über die personenbezogene Daten über das Internet übermittelt werden, z. B. durch Kontaktformulare oder Eingabemasken, werden von uns mit SSL-Zertifikaten geschützt. Die Zertifikate werden in regelmäßigen Abständen neu ausgestellt, um einen Diebstahl des Zertifikats und somit das Abgreifen von Daten zu verhindern.

Integrität

Eingabekontrolle

Bei der Eingabekontrolle soll die Überprüfung, wer, wann, welche Daten und auf welchen Systemen eingegeben und verarbeitet hat, erfolgen. Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme: Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berech-

tigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die diesen eigentlich nicht gestattet wären.

Verwendung personalisierter Logins: Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.

Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle dienen auch der Sicherstellung der Integrität.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Durchführung von Code-Reviews in der Entwicklung: Alle entwickelten Code-Bestandteile werden durch einen zweiten Mitarbeiter mit entsprechenden Fachkenntnissen geprüft. Bevor der jeweilige Code in das Produktivsystem eingespielt wird, muss dieser durch beide Mitarbeiter freigegeben werden. Dieses Vier-Augen-Prinzip stellt sicher, dass Systeme nicht offensichtlichen Fehlern aus gesetzt sind und dass die zuvor definierten Anforderungen an die Qualität des Codes eingehalten werden.

Erstellung von Code-Dokumentationen in der Entwicklung: Alle entwickelten Systeme und darin verwendete Code-Bestandteile werden durch die Entwickler hinreichend dokumentiert. Dies stellt u. A. eine schnelle Einarbeitung anderer Mitarbeiter in das jeweilige Projekt sicher. Darüber hinaus kann eine Weiterentwicklung der jeweiligen Code-Bestandteile zukünftig auch dann erfolgen, wenn der ursprüngliche Entwickler nicht mehr im Unternehmen tätig ist. Durch eine hinreichende Dokumentation wird zudem sichergestellt, dass Bugs oder Fehler schneller identifiziert und behoben werden können.

Klimatisierung von Räumen mit kritischer IT-Infrastruktur: Alle Systemkomponenten, die zur Sicherstellung des Betriebs sowie zur Bereitstellung von Kundensystemen notwendig sind (z. B. Server, Netzwerkkomponenten oder Backup-Systeme) sind vor schädlichen Umgebungsbedingungen wie zu hohen Temperaturen oder zu hoher Luftfeuchtigkeit mittels einer Klimatisierung geschützt. Diese wird regelmäßig gewartet und bei einer Erweiterung der Systemkomponenten entsprechend der benötigten Kühlleistung aus gebaut.

Nutzung einer Versionskontrolle in der Entwicklung: Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z.B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.

Nutzung von Testverfahren in der Entwicklung: Entwickelte Komponenten für interne Systeme sowie für Kundensysteme werden durch spezielle Tests (z. B. Unittests) einer regelmäßigen und automatisierten Prüfung unterzogen. Dabei wird mittels verschiedener Testszenarien sichergestellt, dass auch bei der nachträglichen Einführung von Änderungen an einem System die wesentlichen Kom-

ponenten auf verschiedene Eingaben hin das richtige und zu erwartende Verhalten zeigen. Mögliche Fehler können so frühzeitig erkannt und behoben werden.

Regelmäßige Durchführung von Updates: Alle im Einsatz befindlichen Betriebssysteme sowie darauf installierte Anwendungen und Bibliotheken werden stets aktuell gehalten. Entsprechende Updates werden regelmäßig eingespielt. Zur Verfügung gestellte Security-Patches werden ebenfalls zeitnah eingespielt, um die entsprechenden Sicherheitslücken schnellstmöglich zu schließen. Werden für Anwendungen oder Bibliotheken keine Security-Updates mehr ausgeliefert oder wird die Anwendung vom Hersteller nicht mehr weiterentwickelt oder betreut, findet ein Upgrade auf eine aktuelle Version statt oder es findet ein Wechsel auf eine noch unterstützte alternative Anwendung statt.

Überprüfung erstellter Datensicherungen: Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig aus gewählte Daten von einem zufällig aus gewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.

Verwendung von Brandmeldern: Zur Vermeidung von Schäden durch Feuer werden Brandmelder verwendet. Diese wurden in jedem Bereich der Büroräume angebracht. Im unwahrscheinlichen Fall eines Feuers kann so der betroffene Bereich schnell identifiziert und mit Hilfe von öffentlich zugänglichen Feuerlöschern bei Bedarf gelöscht werden. Die Brandmeldeanlage wird regelmäßig gewartet, um deren ordnungsgemäße Funktion sicherzustellen.

Verwendung einer Firewall: Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Verwendung und regelmäßige Aktualisierung eines Virenscanners: Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch aus gewählte Mitarbeiter möglich.

Verwendung von RAID-Systemen: Zum Schutz vor Hardwareausfällen und Datenverlusten durch defekte Festplatten, werden diese in kritischen IT-Systemen (z. B. lokale Datei- oder Entwicklungsserver) in Form eines RAID-Systems verbaut. In diesem werden Daten auf mindestens zwei Festplatten gespeichert. Auf die in einem RAID- System gespeicherten Daten kann somit auch bei einem Ausfall von einer Festplatte weiterhin zugegriffen werden. Defekte Festplatten werden umgehend vom System gemeldet und können entsprechend getauscht werden. Ein Datenverlust kann s o vermieden werden.

Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen: Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dies er Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Erstellung von Notfallplänen für kritische Prozesse: Für die aus Datenschutzsicht kritischen Prozesse im Unternehmen wurden spezielle Notfallpläne erstellt. Diese beinhalten Informationen zum geplanten Vorgehen in datenschutzrelevanten Notfallsituationen (z. B. Verlust von personenbezogenen Daten). Auch die notwendigen Kommunikationsinhalte, – kanäle und -empfänger werden konkret benannt, um sicherzustellen, das s alle betroffenen Personen zeitnah über den jeweiligen Notfall informiert werden. Welche Prozesse als kritisch einzustufen sind, wurde von allen Datenschutzverantwortlichen im Unternehmen gemeinsam definiert. Eine zukünftige Erweiterung der Notfallpläne wird durch das gleiche Gremium initiiert und durchgeführt.

Nutzung einer Versionskontrolle in der Entwicklung: Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z.B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.

Regelmäßiger Testdurchlauf von Notfallplänen für kritische Prozesse: Für die im Vorfeld definierten kritischen Prozesse im Unternehmen findet regelmäßig ein Testdurchlauf statt. Hierfür wird zu einem zufällig aus gewählten Zeitpunkt ein bestimmtes Szenario definiert und unter realen Bedingungen durchgespielt. Allen beteiligten Mitarbeitern wird mitgeteilt, dass es sich um einen Testdurchlauf handelt, damit keine unerwünschte Kommunikation an Externe (z. B. an Kunden) erfolgt. Auffälligkeiten sowie Optimierungspunkte werden im Nachgang gesammelt und, sofern sinnvoll, direkt umgesetzt.

Überprüfung erstellter Datensicherungen: Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig aus gewählte Daten von einem zufällig aus gewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.

Verwendung einer Firewall: Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Verwendung und regelmäßige Aktualisierung eines Spamfilters: Um Kunden deren Mitarbeiter, für die wir im Rahmen unserer Dienstleistungen auch das E-Mail-Hosting übernehmen, vor Spam-E-Mails und Phishing-E-Mails zu s schützen, kommen spezielle Spamschutzlösungen auf den von uns genutzten Mailservern zum Einsatz. Die zur Erkennung von Spam- und Phishing-E-Mails notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Um die korrekte Funktion des eingesetzten Spam-Filters sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Spamschutzlösungen erkannt wird.

Verwendung und regelmäßige Aktualisierung eines Virenscanners: Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch aus gewählte Mitarbeiter möglich.

Weitere Maßnahmen

Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen: Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dies er Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Jährliche Überprüfung der Wirksamkeit der ergriffenen Schutzmaßnahmen: Unabhängig von zusätzlich durchgeführten externen Security-Audits, erfolgt jährlich eine innerbetriebliche Überprüfung zur Wirksamkeit der ergriffenen technischen und organisatorischen Schutzmaßnahmen. Hierzu werden die aktuellen Schutzmaßnahmen gemeinsam mit Vertretern aller Verantwortungsbereiche beleuchtet und sofern sinnvoll entsprechende Optimierungen festgelegt.

Sichere Entsorgung von gedruckten Dokumenten: Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung, die von einem Spezialunternehmen (z. B. Reisswolf) nachweis lich vernichtet und entsorgt werden.

Sicheres Löschen nicht mehr benötigter Daten: Nicht mehr benötigte Daten, wie zum Beispiel veraltete Kunden- sowie Projektdaten oder Daten aus Test- bzw. Entwicklungsumgebungen, werden gelöscht, sobald diese nicht mehr für die jeweilige Vertragserfüllung benötigt werden. Die Löschung erfolgt unter Zuhilfenahme spezieller Löschprogramme, welche eine nachträgliche Wiederherstellung der Daten unmöglich machen.

Zuteilung von datenschutzrelevanten Verantwortungsbereichen: Datenschutzrelevante Verantwortungsbereiche werden je nach Tätigkeitsbereich auf Mitarbeiter verteilt. Dabei wird die Eignung der Mitarbeiter für den jeweiligen Verantwortungsbereich stets sichergestellt. Ggf. notwendige Schulungen oder Fortbildungen erfolgen vor der Übertragung eines Verantwortungsbereichs an einen Mitarbeiter. Alle datenschutzrelevanten Verantwortungsbereiche werden schriftlich festgehalten und auch in AV-Verträgen mit Endkunden berücksichtigt. Bei Aus tritt eines Mitarbeiters wird unverzüglich ein geeigneter Nachfolger benannt.

Auftragskontrolle

Bei der Auftragskontrolle soll sichergestellt werden, dass der externe Dienstleister die personenbezogenen Daten alleinig nach Weisung des Auftraggebers verarbeitet. Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden: Mit allen Dienstleistern, Partnern und Kunden, mit denen ein Austausch sowie eine Verarbeitung von personenbezogenen Daten erfolgen, wird ein Vertrag zur Auftragsdatenverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO geschlossen. In dem AV-Vertrag werden u. a. die folgenden Aspekte zwischen den beiden Vertragspartnern geregelt: “Anwendungsbereich und Verantwortlichkeit”, “Gegenstand und Dauer des Auftrages ”, “Beschreibung der Verarbeitung, Daten und betroffener Personen”, “Technische und organisa-

torische Maßnahmen zum Datenschutz", "Berichtigung, Einschränkung und Löschung von Daten", "Pflichten des Auftragnehmers ", "Rechte und Pflichten des Auftraggebers ", "Wahrung von Rechten der betroffenen Person", "Kontrollbefugnisse", "Unterauftragsverhältnisse", "Datengeheimnis und Geheimhaltungspflichten", "Haftung" und "Informationspflichten, Schriftformklausel, Rechtswahl". Der AV-Vertrag wird von beiden Vertragsparteien in schriftlicher oder alternativ in digitaler Form geschlossen. Beide Vertragsparteien verpflichten sich zudem, unverzüglich über relevante Änderungen zu informieren, so dass der AV-Vertrag entsprechend geändert und erneut abgeschlossen werden kann.

Aufklärung von Kunden zum Thema Datenschutz: Nach Auftragserteilung klären wir Kunden über die von uns ergriffenen Maßnahmen zum Datenschutz auf und binden diese so gut wie möglich in die entsprechenden Prozesse mit ein. Falls notwendig, empfehlen und installieren wir beim Kunden entsprechende Anwendungen, um einen optimalen Schutz personenbezogener Daten auch Kundenseite zu ermöglichen. So soll ein gleichermaßen hohes Sicherheitsniveau bei beiden Vertragspartnern sichergestellt werden.

Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten: Bei der Beauftragung von Dienstleistern und Partnern erfolgt vorab ein Vergleich möglicher Anbieter unter Datenschutzaspekten. Hierzu holen wir je nach Art und Umfang des Auftrags Informationen zur Verarbeitung von personenbezogenen beim jeweiligen Anbieter ein. Bewertet werden Aspekte wie die Übermittlung von Daten, deren konkrete Verarbeitung sowie die getroffenen technischen und organisatorischen Schutzmaßnahmen. Eine Zusammenarbeit erfolgt ausschließlich mit Dienstleistern und Partnern, die das geforderte Datenschutzniveau glaubhaft sicherstellen können.

Beauftragung zertifizierter Dienstleister und Partner: Eine Zusammenarbeit erfolgt vorzugsweise mit Dienstleistern und Partnern, die über eine nachgewiesene Zertifizierung verfügen. Dies gilt ins besondere dann, wenn die Zertifizierung auf ein hohes Datenschutzniveau schließen lässt, zum Beispiel bei Anbietern von Webhosting-Dienstleistungen. Die Fristen der jeweiligen Zertifizierungen werden kontrolliert und ggf. neue Zertifizierungen von Dienstleistern und Partnern angefordert, sobald diese neu ausgestellt wurden. Erfolgt keine erneute Zertifizierung, so werden zukünftig vorzugsweise andere Dienstleister und Partner beauftragt, die über das jeweilige Zertifikat verfügen.

Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern: Nach vorheriger Anmeldung führen wir stichprobenartige Überprüfungen zum Thema Datenschutz bei unseren Dienstleistern durch. Hierbei überprüfen wir zum einen, ob zugesicherte Datenschutzmaßnahmen wie vertraglich vereinbart durchgeführt werden. Darüber hinaus sprechen wir Empfehlungen für Optimierungen zum Datenschutz aus und unterstützen bei Bedarf bei deren Implementierung.

Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter: Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz in schriftlicher wie persönlicher Form an neue Mitarbeiter kommuniziert. Neben unserem grundsätzlichen Verständnis vom Umgang mit personenbezogenen Daten vermitteln wir auch das notwendige Wissen zur korrekten Anwendung aller technischen und organisatorischen Datenschutzmaßnahmen.

Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz: Unsere Mitarbeiter werden regelmäßig zu relevanten Datenschutzthemen geschult. Dabei werden sowohl Grundlagen aufgefrischt als auch aktuelle Themen sowie rechtliche Änderungen vermittelt. Neben den entsprechenden datenschutztechnischen Kompetenzen soll so eine hohe Sensibilität für den Schutz personenbezogener Daten bei allen Mitarbeitern gefördert werden.

Schriftliche Anweisungen an Dienstleister: Sämtliche Anweisungen für die Verarbeitung von personenbezogenen Daten durch Dienstleister werden schriftlich übermittelt und im persönlichen Gespräch erläutert. Die schriftlichen Anweisungen enthalten Informationen zur Art der personenbezogenen Daten sowie zu deren datenschutzkonformer Verarbeitung. Ebenfalls schriftlich vereinbart wird, wie Daten zwischen den beiden Parteien ausgetauscht werden und was bei datenschutzrelevanten Ereignissen zu tun ist.

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags: Auftragsbezogene Daten mit personenbezogenen Inhalten, die zur Verarbeitung an uns übermittelt werden, werden bei Beendigung des Auftrags gelöscht, sofern diese nicht aus wichtigem Grund behalten werden müssen. Dies kann zum Beispiel dann notwendig sein, wenn sich aus dem Auftrag weitere Folgeaufträge ergeben, für deren vertragliche Umsetzung die Daten noch einmal benötigt werden. Eine ordnungsgemäße Löschung erfolgt dann nach Abschluss des letzten Folgeauftrags.

Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter: Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und dies e ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten. Darüber hinaus wird der Mitarbeiter über mögliche Folgen von Verstößen gegen die Vertraulichkeitsverpflichtung aufgeklärt. Alle in der Verschwiegenheitserklärung vereinbarten Punkte gelten auch über den Zeitraum der Anstellung hinaus .

Stand: 04.12.2019

Cord Media Digital Services
Frank Oschatz
Schwarze-Breite-Str. 11
73760 Ostfildern

Telefon:+49 173 / 89 20 755
Telefax: +49 711 / 90 004 153
info@cordmedia.de
www.cordmedia.de

BW-Bank
BLZ 60050101 • Konto 66 80 462
IBAN DE 53 60050101 0006680462
BIC SOLADEST600

Umsatzsteuer-ID: DE244043427
Steuer Nr. : 59300 / 46410
Betriebsnummer: 93130109

Dienstleisterinfomationen DS-GVO 2019

Angaben zum Unternehmen

Cord Media Digital Services
Frank Oschatz
Einzelunternehmen (Cord Media Digital Services)
Schwarze Breite Str. 11
73760 Ostfildern

Telefon: 0173 / 89 20 755
Telefax: 0711 / 90004153
E-Mail: info@cordmedia.de

Geschäftsführung
Frank Oschatz

IT-Leitung
Frank Oschatz

Verantwortlich für den Datenschutz
Frank Oschatz

Änderung der technischen und organisatorischen Maßnahmen 2019

- Mobilfunkgerät wurde mit Fingerabdrucksensor und 6-stelligen Code ausgestattet
- Sämtliche Server-basierte Analyse-Systeme auf Fremdservern wurde deaktiviert und deren Nutzung eingestellt.
- Datev wurde eingestellt und durch Lex-Office ersetzt.
- Server-Logfiles wurden komplett deaktiviert und werden nur bei einem technischen Fehler oder dem Verdacht auf Hacker-Aktivitäten zugeschaltet.