Bericht betrieblicher Datenschutz

vom 05.03.2019

Mandant:

multi-media-management GmbH
Georgswall 5
30159 Hannover

Tel.: 0511 760 7780
Fax: 0511 760 77877

Beratendes Unternehmen:

List + Lohr Datenschutz und Informationssicherheit GmbH
Zeißstraße 17b
30519 Hannover

Tel.: 0511 - 49 99 99-600
Fax: 0511 - 49 99 99-649

Email: info@datenschutz-hannover.de

Externer Datenschutzbeauftragter:

Michel Weber
weber@list-lohr.de

Inhalt

1. Vorwort

Als externer Datenschutzbeauftragter wirke ich auf die Einhaltung der Datenschutzbestimmungen hin. Im Rahmen meiner Tätigkeit stelle ich den Ist-Zustand der Betriebsabläufe, der EDV und des Netzwerkes dar und prüfe, ob hier die Richtlinien eingehalten werden. Wenn nötig, spreche ich Empfehlungen zur Verbesserung aus.

Für alle Verfahren der Erfassung, Verarbeitung, Übermittlung oder Nutzung von personenbezogenen Daten wird ein Ist-Zustand gezeigt, Folgenabschätzungen vorgenommen und mögliche Verbesserungen empfohlen.

Bei Einführung neuer Verfahren bin ich hierüber vorab zu informieren. Gegebenenfalls wird eine Folgenabschätzung vorgenommen. Ein wesentliches Augenmerk liegt dabei darauf, dass ausschließlich Befugte eine nur auf den Zweck beschränkte Verarbeitung vornehmen können und dass der Eigentümer der Daten sein Selbstbestimmungsrecht auf Auskunft, Berichtigung, Sperrung und Löschung wahrnehmen kann.

Eine Prüfung der technischen und organisatorischen Maßnahmen findet regelmäßig statt.

Für die Geschäftsleitung und die Mitarbeiter bin ich Ansprechpartner in allen Fragen des Datenschutzes.

2. Datenverarbeitung im Unternehmen

2.1. Verpflichtung und Unterrichtung der Mitarbeiter

Insgesamt sind im Unternehmen 9 Mitarbeiter mit Datenverarbeitung befasst. Eine Verpflichtung auf das Datengeheimnis nach § 53 BDSG-neu wurde von allen Mitarbeitern unterzeichnet. Mitarbeiter wurden bereits für die Einhaltung der Datenschutzvorschriften sensibilisiert. Eine Schulung vor Ort ist für Ende März 2019 geplant.

2.2. Auftragsverarbeitung

Mit Kunden und Dienstleistern bestehen Vereinbarungen zur Auftragsverarbeitung. Eine Übersicht aller Auftragsverarbeitungen wurde erstellt.

2.3. Verzeichnis für Verarbeitungstätigkeiten

Es wurde ein Verzeichnis für Verarbeitungstätigkeiten erstellt. Dieses befindet sich aktuell in der inhaltlichen Prüfung durch die Geschäftsführung. Das Verzeichnis wird fortlaufend überprüft und im Bedarfsfall überarbeitet bzw. ergänzt.

2.4. Interne Konzepte, Richtlinien und Vereinbarungen

Es wurde eine IT-Richtlinie sowie ein Datenschutz- und ein Löschkonzept erstellt. Im Zuge der anstehenden Mitarbeiterschulung werden die Mitarbeiter über die Inhalte der IT-Richtlinie aufgeklärt. Anschließend soll diese von jedem Mitarbeiter unterzeichnet werden.

3. Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Im Unternehmen wurden nachfolgende technische und organisatorische Maßnahmen umgesetzt.

3.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Sicherheitsschlüssel
- Einbruchshemmende Türen und Fenster
- Schlüsselverzeichnis und Schlüsselregelung
- Sorgfältige Auswahl von Reinigungspersonal und externen Dienstleistern
- Protokollierung von Besuchern, Begleitung durch eigene Mitarbeiter

3.2. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Einsatz einer zentralen Hardware-Firewall
- Zugang zu Computern nur mit gültigem Benutzerkonto/Passwort
- Individuelle, geheime und komplexe Passwörter
- Vermeidung von der Wiederholung von Passwörtern für andere Dienste/Anwendungen
- Einsatz von Anti-Viren Software
- Remote-Zugang durch VPN-Tunnel mit zentraler Anmeldung
- Automatisierte Sperrung des Bildschirms
- Prozesse für Rechtevergabe/-entzug bei Eintritt, Veränderung und Austritt von Mitarbeitern
- Verpflichtung auf das Datengeheimnis gem. § 5 BDSG

3.3. Zugriffskontrolle

Maßnahmen, 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:

- Berechtigungskonzept und individuelle Vergabe von Benutzerrechten
- Für die Berechtigungen auf Ordner wird das Need-To-Know-Prinzip angewandt
- Erteilung und Nutzung von Administratorenrechten auf das Notwendigste begrenzt
- Überprüfung der Zugriffsberechtigung
- Konzept zur Laufwerksnutzung und –Zuordnung
- Bestandskontrolle für mobile Datenträger
- Datenschutzkonforme Vernichtung von Datenträgern und vertraulichen Unterlagen

3.4. Weitergabekontrolle

Maßnahmen, 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:

- Einsatz der Systeme nur im privaten Netzwerk oder über verschlüsselte Verbindungen in öffentlichen Netzwerden (VPN-Tunnel)
- E-Mail-Richtlinie bzw. kein Versand personenbezogener Daten per E-Mail
- Unterlagen und Speichermedien werden datenschutzkonform versandt
- Keine Einsicht auf Bildschirme von außerhalb des Gebäudes möglich
- Sorgfältige Auswahl von Transportpersonal-/Fahrzeugen bzw. sichere Verpackungen

3.5. Eingabekontrolle

Maßnahmen, 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:

- Organisatorische Festlegung der Zuständigkeiten für die Eingabe, Zugriffsrechte
- Protokollierung von Eingaben/Änderungen/Löschungen
- Sicherung mehrerer Versionssätze im Rahmen des Backups
- Kontrolle der Dateneingabe

3.6. Auftragskontrolle

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

- Sorgfältige Auswahl geeigneter Dienstleister
- Zentrale Erfassung vorhandener Dienstleister
- Regelmäßige Überprüfung der Eignung der Dienstleister
- Bestellung Datenschutzbeauftragter
- Abschluss von Verträgen zur Auftragsdatenverarbeitung
- Schriftliche Weisungen und Festlegung der Zuständigkeiten, Kontrollrechte
- Sichtung vorhandener IT-Sicherheitszertifikate
- Festlegung zur Vernichtung von Daten nach Ende des Auftragsverhältnisses

3.7. Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Einsatz von Rauchmeldern und Feuerlöschern
- Spiegelung von Festplatten
- Redundante Sicherung von Daten und Systemen
- Verpflichtung auf das Datengeheimnis gem. § 5 BDSG
- Regelmäßige Überprüfung der Wiederherstellbarkeit
- Einsatz von Firewall, Virenscanner, Spam-Filter und automatischen Produkt-Updates

3.8. Trennungsgebot

Maßnahmen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung von Speicherbereichen nach Kunden und Projekten
- Separierung von Dateien bei Datenbanken
- Logische Datentrennung nach Kunden-/Mandantennummern
- Trennung von Entwicklungs-, Test- und Produktivsystemen

4. Datenschutz-Kontrolle / Audit

4.1. Vor-Ort-Kontrolle

Am 28.01.2019 wurde die Ist-Situation in einem Datenschutz-Meeting (Teilnahme: Herren Borchers, Heermann, Weber) erörtert. Im Nachgang wurde eine vor-Ort-Begehung durchgeführt, in der u.a. die Umsetzung der technischen und organisatorischen Maßnahmen geprüft wurde.

4.2. Geplante Maßnahmen

Aus dem Meeting und der Begehung wurden nachfolgende Maßnahmen abgeleitet:

- Prüfung der Zugangsberechtigung für den gemeinsam genutzten Serverraum sowie ggf. Verpflichtung zugangsberechtigter Dritter.
- Prüfung der Sicherheitssoftware für Tablets und Diensthandys (u.a. Container-Lösung).

5. Anfragen und Datenschutz-Vorfälle

Seit Aufnahme der Tätigkeit als externer Datenschutzbeauftragter der multi-media-management GmbH sind keine Anfragen und keine Beschwerden von Betroffenen eingegangen. Besondere Datenschutz-Vorfälle oder Datenpannen gab es bis dato nicht.

6. Bewertung und Ausblick

Die Ist-Situation hinsichtlich der Datenschutz-Konformität bei der multi-media-management GmbH kann insgesamt als gut bezeichnet werden. Im Zuge der Tätigkeit als externer Datenschutzbeauftragter wurden bereits zahlreiche Maßnahmen zu Datenschutz und Informationssicherheit umgesetzt. Routinemäßig werden Mitarbeiter sensibilisiert sowie der aktuelle Handlungsbedarf in Abstimmungsmeetings besprochen. Weitere Maßnahmen sind geplant bzw. in Vorbereitung.