media group

Datensicherheitskonzept

Zutrittskontrolle

1. Unbefugte werden durch Schlüsselvergabe daran gehindert, die Räume des Unternehmens zu betreten und damit an die Datenverarbeitungsanlagen zu gelangen.
2. Die Schlüssel werden nach Funktion und Verantwortungsbereich getrennt vergeben. Der Bereich Lettershop ist nur durch die zugeordneten Mitarbeiter betretbar.
3. Besucher dürfen sich nur unter Aufsicht innerhalb der Firmenräumlichkeiten aufhalten.
4. Der Anlieferungsbereich ist Videoüberwacht.
5. Die Türen zu IT-Systemräumen sind verschlossen.

Zugangskontrolle

1. Der Zugang zum Arbeitsplatzrechner wird durch Passwörter geregelt. Die Passwörter werden entsprechend den Vorgaben der Datenschutzbeauftragten vergeben.
2. In der Datenbank und auf Servern werden alle Benutzer zentral verwaltet. Nur der Administrator hat Zugang zur Benutzerverwaltung. Dort werden die verschiedenen Berechtigungen erstellt und Mitarbeitern zugeteilt.
3. Datenbanknutzer müssen sich unter Angabe von Benutzerkennung und mit Passwort anmelden.
4. Die Mitarbeiter sind angewiesen, in regelmäßigen Abständen ihr Passwort zu wechseln. Dabei muss eine Länge von mindestens 6 Zeichen und eine Kombination aus Buchstaben, Zahlen eingehalten werden.
5. Bei Verlassen des Arbeitsplatzes sind die Mitarbeiter verpflichtet, den Rechner zu sichern und sich bei Wiederaufnahme der Arbeit unter Eingabe ihres Passworts erneut anzumelden.

Zugriffskontrolle

1. In der Datenbank wird das Lesen, Kopieren, Ändern oder Löschen von Daten seitens nicht autorisierter Personen durch Benutzerkonten mit unterschiedlichen Rechten verhindert.
2. Die Zeiten des Ein- und Ausloggens in die Datenbank werden mit Angabe des Benutzernamens protokolliert.
3. Papierausdrucke mit personenbezogenen Daten werden in speziellen Behältern gesammelt und durch einen zertifizierten Entsorgungsbetrieb rückinformationssicher vernichtet.

Weitergabekontrolle

1. Personenbezogene Daten werden in der Datenbank gespeichert und grundsätzlich nur an auftragsbezogene Mitarbeiter/innen weitergegeben.
2. Ein Datenaustausch findet nur mit dem Kunden und nur mit dessen Einverständnis auf elektronischem und postalischem Weg statt.
3. Die Datenbank verlässt die Firmenräumlichkeiten nur als Band- Sicherungskopie durch eine dafür zuständige Person.

Eingabekontrolle

Das Erstellen, die Änderung und das Entfernen von Daten in der Datenbank werden protokolliert. Dabei werden die Person und das Datum festgehalten.

media group

Auftragskontrolle

Bei der Verarbeitung von personenbezogenen Daten im Rahmen einer Auftragsdatenverarbeitung wird sichergestellt, dass die Datenverarbeitung auf Weisung des Kunden stattfindet und nur im Rahmen dieser Weisungen stattfindet.
Eine darüber hinaus gehende unbefugte Datenverarbeitung ist den Mitarbeiter/innen vertraglich durch eine schriftliche Datenschutzvereinbarung untersagt.
Der Inhalt der Weisungen eines Kunden wird den mit der im Rahmen des jeweiligen Auftraggebers betrauten Mitarbeiter/innen verbindlich mitgeteilt.

Verfügbarkeitskontrolle

1. Personenbezogene Daten, die in der Datenbank gespeichert sind, werden durch täglich erstellte Backups gesichert. Die täglich erstellte Sicherungskopie wird in einem anderen Brandabschnitt gelagert.
2. Alle Arbeitsplatzrechner sind durch eine Hardware Firewall vor Angriffen von außen geschützt. Alle Rechner werden durch entsprechende Software vor Schadprogrammen und Viren geschützt.
3. Die Server sind durch eine Unterbrechungsfreie Stromversorgung (USV) vor Ausfall geschützt. Der Serverraum ist klimatisiert.

Trennungskontrolle

Daten die einer Trennpflicht unterliegen, werden logisch getrennt voneinander in verschiedenen Tabellen gespeichert.
Aufgabe ist die Erstellung von Drucksachen (personalisiert / nicht personalisiert), Versandfertig machen (konfektionieren) und versenden im Auftrag des Kunden

Organisationskontrolle

1. Ein externer Datenschutzbeauftragter mit Nachweis der nötigen Fachkunde wurde schriftlich bestellt.
2. Das öffentliche Verfahrensverzeichnis liegt vor und kann auf Anfrage zur Verfügung gestellt werden.
3. Die Mitarbeiter werden regelmäßig auf den Datenschutz sensibilisiert und geschult.

Öffentliches Verfahrensverzeichnis

Der Schutz Ihrer persönlichen Daten und Ihrer Privatsphäre ist uns sehr wichtig. Deshalb ist die Beachtung der Bestimmungen des Bundesdatenschutzgesetzes (BDSG) für uns selbstverständlich. Zweck dieses Gesetzes ist es, Sie davor zu schützen, dass Sie durch die Nutzung Ihrer personenbezogenen Daten durch andere in Ihrem Persönlichkeitsrecht beeinträchtigt werden. Da Sie ein Recht auf Auskunft über jegliche Nutzung Ihrer Daten haben, informieren wir Sie hiermit in Anlehnung an die §§ 4 ff BDSG (Verfahrensverzeichnis).

Selbstverständlich können Sie der Nutzung Ihrer Daten widersprechen, sofern diese nicht für die Abwicklung eines Vertrags- bzw. Beteiligungsverhältnisses erforderlich sind. Für einen solchen Widerspruch genügt eine E-Mail von Ihnen an raff@walliser-datenschutz.de. Sie erhalten dann eine Bestätigung auf demselben Kommunikationsweg, sobald der Widerspruch ins System eingepflegt ist.

Für weitere Fragen steht Ihnen unser Datenschutzbeauftragter gerne zur Verfügung. (Kontaktdaten unter Punkt 2)

Verfahrenskontrolle

1. Verantwortliche Stelle:
   raff digital gmbh, Amtsgericht Stuttgart HRB 361302, Dieter Raff (Geschäftsführer)
2. Inhaber:
   Jens Reutter (IT-Verantwortlicher)

   Der Verantwortliche für die Datenverarbeitung:
   Dipl.-Ing. Matthias Walliser (bestellter externer Datenschutzbeauftragter)
   raff@walliser-datenschutz.de

   Die zuständige Aufsichtsbehörde
   Der Landesbeauftragte für den Datenschutz Baden-Württemberg
   Urbanstr. 32, 70182 Stuttgart, Telefon 0711 61 55 41-0, Telefax 0711 61 55 41-15
   E-Mail: poststelle@lfd.bwl.de, www.baden-wuerttemberg.datenschutz.de
3. Anschrift der verantwortlichen Stelle
   raff media group gmbh, Industriestr. 14, 72585 Riederich, Telefon +49 (0)7123 3815-912
   E-Mail: info@raff-mediagroup.de, www.raff-mediagroup.de

4. Zweckbestimmung
   Gegenstand des Geschäftsbetriebs der raff digtal gmbh (kurz: raff digtal) ist die Herstellung von Druck und Verlagserzeugnissen einschließlich Prepress und Postpress, sowie der Handel Medienerzeugnissen und ähnlichen Produkten.

   Nebenzwecke sind begleitende oder unterstützende Funktionen wie im Wesentlichen die Personal-, Vermittler-, Lieferanten- und Dienstleisterverwaltung. Durchführung der Speicherung und Datenverarbeitung von personenbezogenen Daten für eigene Zwecke.

   Zu diesem Zweck ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Geschäftspartner (Adressdaten, einschl. Telefon-, Fax- und E-Mail-Daten, Auskünfte, Bankverbindungen) im Rahmen eines ordnungsgemäßen Geschäftsbetriebs nach §28 BDSG notwendig.

   Hierzu beschäftigt die raff digital Personal im Rahmen von festen Arbeitsverträgen als auch freie Mitarbeiter, die im Auftrag der raff digital Dienstleistungen erbringen. raff digital erhebt, verarbeitet und nutzt zu diesem Zweck personenbezogene Daten ihrer Mitarbeiter und für die Dauer von Bewerbungsverfahren personenbezogene Daten der Bewerber.
   Des Weiteren werden personenbezogene Daten auch im Rahmen von Partnerschaften erhoben, verarbeitet und genutzt. Insbesondere zählen hierzu die Gesellschaften im Verantwortungsbereich der Holding, Daten nach gesetzlichen Vorgaben und Vertragsvereinbarungen mit Sozialleistungsträgern (z.B. Krankenkassen) sowie Verbänden.
5. Betroffene Personengruppen und der diesbezüglichen Daten oder Datenkategorien
   Es werden im Wesentlichen zu folgenden Gruppen personenbezogene Daten erhoben, verarbeitet und genutzt, soweit es sich um natürliche Personen handelt und soweit diese zur Erfüllung der oben genannten Zwecke erforderlich sind.

   Angestellte Mitarbeiter:
   - Personalien (Name, Anschrift, Geburtsdatum, Familienstand, Staatsangehörigkeit, Bankverbindung, Beruf/Branche und Konfession)
   - Dienstbezogene Daten für Mitarbeiter (Ausbildung, Dienstzeiten, Ausfallzeiten, Urlaub, Ein- Austrittsdatum, etc.)
   - Einkommensdaten (Lohn, Gehalt, sonstige Einkünfte, Pfändungen)

Geschäftspartner:
- Adressdaten, Funktionsdaten und Bankverbindungen
  Kontaktpersonen der vorgenannten Gruppen:
  (auch falls es sich dabei um juristische Personen handelt):
- Kontaktdaten

Videoüberwachung:
- Außenbereiche und Zufahrten zum Firmengelände

6. Regelfristen für die Löschung der Daten
   - Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen, die im Wesentlichen eine Aufbewahrungsfrist von 10 Jahren erfordern, zum Teil aber auch darunter liegen. Darüber hinaus können sich Abweichungen durch satzungsmäßige oder vertragliche Aufbewahrungsfristen ergeben.
   - Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Vertragserfüllung (z.B. bei Werk- und Dienstverträgen) erforderlich sind.
   - Sollte eine Löschung aus technischen oder organisatorischen Gründen nicht möglich sein, werden Ihre Daten für eine weitere Verarbeitung und Nutzung gesperrt.

   Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn die Zweckbestimmung entfällt.

7. Datenübermittlung ins Ausland
   - Eine Übermittlung von personenbezogenen Daten in Drittstaaten findet derzeit nicht statt.
   - Es erfolgt dann eine Übermittlung, wenn diese zur Kommunikation mit dem Vertragspartner, in seinem Auftrag oder zur Vertragserfüllung erforderlich ist.

8. Sicherheitsmaßnahmen nach §9 BDSG + Anlage
   Wir haben eine Vielzahl von Vorkehrungen zum Schutz Ihrer Daten getroffen. Die Darlegung von Einzelheiten wäre kontraproduktiv, weil damit zugleich die Struktur an sich wieder angreifbar gemacht würde. Deshalb sieht der Gesetz- geber nach BDSG in Ihrem Interesse vor, dass Angaben zu den technischen und organisatorischen Einzelmaßnahmen nicht öffentlich zur Verfügung gestellt werden.

   Wir versichern Ihnen jedoch, dass wir vielfältige Maßnahmen, entsprechend einem Unternehmen unserer Größenordnung, nach folgenden Erfordernissen des §9 BDSG getroffen haben und diese regelmäßig kontrollieren und nach dem aktuellen Stand der Technik optimieren:

   - Zutrittskontrolle
   - Zugangskontrolle
   - Zugriffskontrolle
   - Weitergabekontrolle
   - Eingabekontrolle
   - Auftragskontrolle
   - Verfügbarkeitskontrolle
   - Trennungsgebot