ROEDIG PARTNER
Agentur für Absatzmarketing und Event

Öffentliches Verfahrensverzeichnis

Das Bundesdatenschutzgesetz (BDSG) schreibt im § 4g vor, dass der Beauftragte für den Datenschutz auf Antrag jedermann die Angaben entsprechend § 4e BDSG in geeigneter Weise verfügbar zu machen hat:

1. Name und Anschrift der verantwortlichen Stelle i.S.d BDSG

ROEDIG GmbH
Römerstraße 75, 71229 Leonberg

Registergericht: Amtsgericht Stuttgart HRB 721971
Umsatzsteuer-Identifikationsnummer: DE 25314 / 3345

Fon 07152 / 33 111 - 0
Fax 07152 / 33 111 - 10
Web http://www.roedig-partner.de
Email kontakt@roedig-partner.de

2. Geschäftsführer:

Sven Rödig
Thomas Bruker

3. Beauftragter Leiter für die Datenverarbeitung

Christoph Feeser

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Der Tätigkeitsbereich der ROEDIG GmbH liegt in der Konzeption und Umsetzung von marketingpolitischen Maßnahmen, insbesondere in den Bereichen Absatzmarketing, Messe und Event. Die hohen Ansprüche an die Qualität der angebotenen Produkte und Dienstleistungen gelten in gleichem Maße für die Einhaltung der Bestimmungen des Datenschutzes. Im Zusammenhang mit den Tätigkeitsfeldern ergeben sich spezielle gesetzliche und datenschutzrechtliche Verpflichtungen. Die Datenerhebung, -verarbeitung und -nutzung erfolgt hauptsächlich im Rahmen der Abwicklung oder Akquise von Aufträgen zur Ausübung der genannten Zwecke. Im Personalwesen erfolgt die Datenerhebung, -verarbeitung und -nutzung sowie gegebenenfalls die Datenübermittlung von personenbezogenen Daten für eigene Zwecke (Personalverwaltung, Zeiterfassung, Bewerbermanagement, betriebliche Altersversorgung, Gehaltsabrechnung, Dienstreisemanagement) oder zur Erfüllung sozialversicherungsrechtlicher und sonstiger gesetzlicher Verpflichtungen.

5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten und Datenkategorien

Betroffene Personengruppen sind:

- **Auftraggeber / Kunden**
  Adressdaten (inkl. Telefon, Fax und Email), Bankverbindungen
- **Interessenten / Nichtkunden**
  Adressdaten, Angebots-, Abrechnungs- und Leistungsdaten
- **Auftragnehmer / Lieferanten**

- Adressdaten (inkl. Telefon, Fax und Email), Bankverbindungen,
- Vertrags-, Abrechnungs- und Leistungsdaten
- **Bewerberdaten**
  Bewerbungsunterlagen, beruflicher Werdegang, Ausbildung, Qualifikation
- **Mitarbeiterdaten**
- Vertrags-, Stamm- und Abrechnungsdaten (soweit für Sozialleistungen relevant), Lohnsteuerdaten, Bankverbindungen, Daten zur Personalverwaltung und -steuerung

sofern diese zur Erfüllung der unter 4. genannten Zwecke erforderlich sind.

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

Mögliche Empfänger / Kategorien von Empfängern:

- Öffentliche Stellen bei Vorliegen vorrangiger Rechtsvorschriften
- Interne Stellen, die an der Ausführung der entsprechenden Geschäftsprozesse beteiligt sind (Personalverwaltung, Buchhaltung, Rechnungswesen, Einkauf, Marketing, Verwaltung, Vertrieb und EDV)
- Externe Auftragnehmer gem. §11 BDSG (Auftragsdatenverarbeitung)
- Externe Stellen und interne Abteilungen der ROEDIG GmbH

zur Erfüllung der unter Punkt 4 genannten Zwecke.

7. Regelfristen für die Löschung von Daten

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen können die entsprechenden Daten gelöscht werden, wenn sie nicht mehr zur Vertragserfüllung oder für unternehmerische Zwecke erforderlich sind, sowie auf Grund von gesetzlichen Erfordernissen notwendig sind.

8. Geplante Übermittlung an Drittstaaten

Eine Übermittlung an Drittstaaten ist derzeit nicht geplant. Im Falle einer Übermittlung in Drittstaaten werden die entsprechenden rechtlichen Voraussetzungen nach dem gültigen Bundesdatenschutzgesetz (BDSG) in seiner jeweiligen aktuellen Fassung geschaffen und eingehalten. Datenübermittlungen in Länder außerhalb der EU bzw. des EWR ergeben sich ausschließlich im Rahmen der Vertragserfüllung, erforderlicher Kommunikation sowie anderer im BDSG ausdrücklich vorgesehener Ausnahmen.

9. Technische und Organisatorische Maßnahmen gem. §9 BDSG

Die Firma ROEDIG GmbH trifft technische und organisatorische Maßnahmen gemäß BDSG §9 um gespeicherte personenbezogene Daten und Informationen zu schützen. Diese sind nachfolgend auszugsweise dargestellt.

Zutrittskontrolle

Die Geschäftsräume der ROEDIG GmbH befinden sich im zweiten und neunten Stock innerhalb eines Bürokomplexes, der durch technische Alarmsysteme gesichert ist. Die Geschäftsräume sind nur über den hauseigenen Aufzug zu erreichen. Im Haus befinden sich 12 Parteien, jeweils 2 Parteien teilen sich eine Etage. Der Haupteingang des Bürogebäudes ist an Wochentagen von 09:00 Uhr bis 18:00 Uhr geöffnet, außerhalb dieser Zeiten ist der Zutritt nur über die Schließanlage möglich. Ein externer Wachdienst ist mit der Sicherung des Gebäudes beauftragt.

Die Büroräume der ROEDIG GmbH sind durch eine Schließanlage vor unbefugtem Zutritt geschützt. Die Schlüsselregelung ist einem Schlüsselbuch dokumentiert. Die Eingangstüren zu den Büroräumen sind feuerhemmende Türen aus massivem Holz. Besucher melden sich im Empfangsbereich an und werden stets während ihrer Anwesenheit von einem Mitarbeiter begleitet. Fremde dürfen sich in den Geschäftsräumen niemals alleine aufhalten oder bewegen. Auf Grund der Unternehmensgröße sind alle Mitarbeiter gegenseitig bekannt. Für die Identifikation von Besuchern steht zudem eine Klingel mit Gegensprechanlage bereit. Es besteht stets Sichtkontakt zum Haupteingang. Der Zutritt über Fenster oder Fluchtwege von außen ist nicht möglich.

Zugangskontrolle

Jeder Mitarbeiter verfügt über eine User ID und ein Passwort. Passwörter müssen in einem regelmäßigen Turnus von 180 Tagen gewechselt werden.

Mindestanforderungen an Passwörter und Passwortsicherheit:
Mindestlänge: 8 Zeichen. Passwörter müssen Zahlen, Ziffern und Sonderzeichen enthalten. Die Mindestanforderungen sind systemseitig festgelegt und können nicht umgangen werden. Es existieren keine Gruppenpasswörter. Unzulässige Authentifikationen führen zur unbefristeten Sperrung des Accounts. Eine unzulässige Authentifikation liegt bei dreimaliger Falscheingabe des Passworts vor. Gesperrte Accounts können nur vom Administrator entsperrt werden.

Regeln für einen sicheren Umgang mit Passwörtern:
- Passwörter dürfen nicht aufgeschrieben, auf den Monitor oder die Tastatur geheftet werden.
- Bei der Eingabe des Passwortes ist darauf zu achten, dass niemand zusieht.
- Passwörter dürfen nicht auf den lokalen Computern gespeichert werden.
- Passwort dürfen nicht per E-Mail verschickt werden.

Sperrung der DV Stationen bei Abwesenheit:
Die Mitarbeiter sind angehalten, die Bildschirmsperre ihrer DV Station bei Abwesenheit zu aktivieren. Dies gilt auch bei nur kurzzeitiger Abwesenheit. Sollte die Bildschirmsperre versehentlich nicht manuell aktiviert werden, erfolgt die Sperrung nach fünf Minuten automatisch.

Sensible DV Systeme
Der Zugang zu den eingesetzten Serversystemen im Unternehmen kann nur durch einen Admin oder, im Bedarfsfall, die Geschäftsführung erfolgen.

Zugriffskontrolle

Über die systemeigene Verwaltung werden Zugriffe auf DV Stationen protokolliert und können im Bedarfsfall ausgewertet werden. Die Systeme sind durch technische Maßnahmen, wie ein aktuelle Firewall und Virenscanner, vor Zugriffen von außen geschützt.

Der Zugriff auf bestimmte Laufwerke oder Ordner wird anhand von NTFS-Rechten geregelt. Mitarbeiter erhalten von der IT Zugriffsrechte auf Daten, die zur Erfüllung Ihres Aufgabenbereichs notwendig sind.

Zugriff auf personenbezogene Daten
Personenbezogene Daten sind besonders schützenswert und vor Einsicht und Zugriff durch Dritte zu schützen. Hierzu zählen neben Kundendaten insbesondere Daten zum Gehalt und Daten zur Arbeitszeit. Die Mitarbeiter sind dazu angehalten sicherzustellen, dass unberechtigte Einblicke oder Zugriffe mit geeignete Maßnahmen zu verhindern.

Weitergabekontrolle

Es wird Sorge getragen, dass personenbezogene Daten in den Softwareprogrammen bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Datenaustausch erfolgt verschlüsselt. Die Übertragungswege sind passwortgeschützt. Mobile Datenträger mit personenbezogenen Daten werden nur in gesicherten Räumen gehalten.

Eingabekontrolle

Mit der Eingabekontrolle soll sichergestellt werden, dass auch im Nachhinein überprüft werden kann, ob und durch wen personenbezogene Daten in Datenverarbeitungsprogramme eingegeben, verändert oder gelöscht worden sind. Technisch erfolgt die Eingabekontrolle durch systemseitige Protokollierung der An- und Abmeldungen. Anhand von Historien kann nachvollzogen werden, welche Benutzer ID an der Eingabe beteiligt war. Die Mitarbeiter sind zudem dazu angehalten, wichtige Eingaben zu protokollieren.

Auftragskontrolle

Die Datenverarbeitung durch Dritte (im Auftrag) erfolgt, insofern diese notwendig wird, mit entsprechenden Verträgen und Weisungen abgesichert und erfolgt unter Berücksichtigung von §11 BDSG. Der Datenschutzbeauftragte hat die vertraglich zugesicherte Möglichkeit, die technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überprüfen.

Adressdaten werden nur entsprechend den Weisungen des Auftraggebers verarbeitet. Insbesondere unterliegen Anweisungen zu Aufträgen oder Bestellungen der Schriftform und diese werden unter Vergabe einer eindeutigen Auftragskennung je Auftrag / Kunde vollständig dokumentiert sowie die Ausführung protokolliert. Der Versand von Daten erfolgt nur mit Angaben, die zur klaren Identifikation erforderlich sind.

Verfügbarkeitskontrolle

Tägliche Datensicherungen garantieren, dass bei Verlust der Funktionsfähigkeit von EDV-Systemen keine Daten verloren gehen. Neben einer wöchentlichen Sicherung auf Bandspeichern, findet eine tägliche Sicherung auf magnetischen Datenträgern statt. Für den Fall von Feuer oder anderen EDV-System schädigenden Ereignissen ist die Datensicherung auch außerhalb des Serverraumes gelagert.

Trennungsgebot

Durch die Trennung der Aufträge voneinander die sowohl in getrennten Auftragsmappen als auch in voneinander getrennten Netzwerkverzeichnissen erfolgt, ist gewährleistet, dass zu unterschiedlichen Zwecken erhobene Adressdaten getrennt verarbeitet werden.

10. Datenschutzbeauftragter

Externer Datenschutzbeauftragter: Fabian Henkel
Stellvertreter im Unternehmen: Martin Grözinger