Checkliste für die Prüfung von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung

Erstprüfung und Folgeprüfung

Zentrale
rocom GmbH | Eichenstraße 8a | 83083 Riedering | www.rocom.de
Tel: +49 (0) 80 36-67482-0 | Fax: +49 (0) 80 36-67482-10 | info@rocom.de
Büro Berlin
Ekkehardstraße 3 | 12437 Berlin | Tel: +49 (0) 30-92 15 21 01
Geschäftsführer: Jens-Peter Riedl | Amtsgericht Traunstein HRB 8452
Raiba Rosenheim | IBAN: DE23 7116 0000 0005 904 41 | BIC: GENODEF1VRR

1. Gesetzliche Grundlagen zu technisch organisatorischen Maßnahmen

1.1 § 9 BDSG – „Technische und organisatorische Maßnahmen“

Öffentliche und nicht-öffentliche Stellen, 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 dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Anlage zu § 9 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind:

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. 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 von personenbezogenen Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in
Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind
(Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. (Trennungsgebot)

2 Angaben zum Datenschutzbeauftragten des Auftragnehmers

Name	Svetlana Riedl
Firma	rocom GmbH
Anschrift	Eichenstrasse 8a, 83083 Riedering
Kontaktdaten	08036 / 67482-0
Ausbildung	Informatikkauffrau
Weiterbildung im Bereich Datenschutz	14.10.2013 – 18.10.2013

3 Durch wen erfolgte die Prüfung des Auftragnehmers?

Name	Michael Wüstendörfer
Firma	rocom GmbH
Anschrift	Eichenstrasse 8a, 83083 Riedering
Kontaktdaten	08036 / 67482-21
Ausbildung	Master Sozialmanagement

4 Wer wurde beim Auftragnehmer befragt?

Name	Michael Wild
Firma	rocom GmbH
Anschrift	Eichenstrasse 8a, 83083 Riedering
Kontaktdaten	08036 / 67482-92
Ausbildung	Dipl.-Inform. (FH)
Funktion und Verantwortung im Unternehmen des Auftragnehmers?	Leitung EDV

Name	Jens-Peter Riedl
Firma	rocom GmbH
Anschrift	Eichenstrasse 8a, 83083 Riedering
Kontaktdaten	08036 / 67482-22
Ausbildung	Dipl.-Inform. (FH)
Funktion und Verantwortung im Unternehmen des Auftragnehmers?	Geschäftsführer

5 Wie erfolgt die Erstkontrolle?

Prüfung	**Wann?**
Vor Ort / telefonisch / schriftlich	14.05.2018

6 Freigabe der Auftragsdatenverarbeitung

Verantwortlicher	**Name / ggf. Unterschrift**
Datenschutzbeauftragter	Svetlana Riedl
Anderer Verantwortlicher	Jens-Peter Riedl
Freigabe erteilt?	Ja / Nein
Bemerkung	Die mit „Nein“ beantworteten Punkte werden nachgearbeitet.
Datum	14.05.2018
Nächste Prüfung?	14.05.2020

7 Erneute Kontrolle

Verantwortlicher	**Name / ggf. Unterschrift**
Datenschutzbeauftragter	Svetlana Riedl
Anderer Verantwortlicher	Jens-Peter Riedl
Freigabe erteilt?	Ja / Nein
Bemerkung	Die mit „Nein“ beantworteten Punkte werden nachgearbeitet.
Datum	14.05.2020
Nächste Prüfung?	14.05.2021

8. Datenschutzaudit

Organisationskontrolle	Ja	Nein
Datenschutzbeauftragter vorhanden (§§ 4f, 4g BDSG)	☒	☐
Mitarbeiter zum Datengeheimnis nach § 5 BDSG verpflichtet?	☒	☐
Mitarbeiterschulung zum Datenschutz erfolgt?	☒	☐
Datenschutzkonzept erarbeitet?	☒	☐

Zutrittskontrolle	Ja	Nein
Zutritt zum Gebäude beschränkt?	☒	☐
Erfolgt eine Besucherkontrolle?	☒	☐
Besteht eine Videoüberwachung?	☒	☐
Rechnerräume nur für befugtes Personal zugänglich?	☒	☐
Server sicher aufgestellt?	☒	☐
Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird (Akten, Datenträger)?	☒	☐

Zugangskontrolle	Ja	Nein
Bildschirmsperren eingerichtet?	☒	☐
Firewall installiert, aktiviert, aktualisiert?	☒	☐
Benutzeridentifikation/Authentifizierung eingerichtet?	☒	☐
Sichere Passwörter?	☒	☐

Zugriffskontrolle	Ja	Nein
Konzept für Zugriffsberechtigungen liegt vor?	☒	☐
Unterschiedliche Zugriffsrechte eingeteilt?	☒	☐
Verletzungen werden protokoliert?	☒	☐
Datenträger/Datenblätter werden sicher entsorgt?	☒	☐
Kopierschutz/Bearbeitungsschutz eingerichtet?	☐	☒

Weitergabekontrolle	Ja	Nein
Datenverschlüsselung eingerichtet und aktiv?	☒	☐
regelmäßige Wartung und Prüfung der Datenverarbeitungssysteme?	☒	☐
Veraltetes Equipment sicher entsorgt?	☒	☐
Beschränkung der Nutzung von privatem Equipment?	☐	☒

Eingabekontrolle	Ja	Nein
Protokollierung von Erhebungen, Änderungen und Löschung?	☒	☐
Protokollierung von Verwaltungsakten?	☐	☒
Besteht eine regelmäßige Protokollkontrolle und - auswertungen bei Änderungen an Daten des Auftraggebers?	☒	☐
Besteht eine schriftliche Dokumentation der Verfahren bei denen Daten des Auftraggebers verarbeitet werden?	☐	☒

Auftragskontrolle	Ja	Nein
Existieren datenschutzgerechte Verträge nach § 11 BDSG zwischen Auftraggeber und Auftragnehmer?	☒	☐
Bestehen Kontrollrechte des Auftraggebers beim Subunternehmer des Auftragnehmers?	☒	☐
Konfliktmanagement bei Verstößen/Verdachtsfällen installiert?	☐	☒
Mechanismen zur Selbstkontrolle auf Seiten des Auftragnehmers vorhanden?	☒	☐

Verfügbarkeitskontrolle	Ja	Nein
Daten gegen unbeabsichtigte Löschung oder Vernichtung abgesichert?	☒	☐
Besteht ein ausreichender Virenschutz bei Auftragnehmer?	☒	☐
Besteht ausreichender Firewallschutz bei Auftragnehmer?	☒	☐
Bestehen ein Datensicherungskonzept und eine Dokumentation der Datensicherung?	☒	☐
Sicherungskopien vorhanden?	☒	☐
Werden regelmäßig Rücksicherungen getestet?	☒	☐
Werden die Systeme des Auftragnehmers regelmäßig mit Sicherheitsupdates versehen?	☒	☐
Besteht eine unterbrechungsfreie Stromversorgung?	☒	☐

Trennungsgebot	Ja	Nein
Besteht eine Trennung von Entwicklungs-, Test- und Produktivsystem?	☒	☐
Erfolgt eine Trennung der Daten des Auftraggebers von eigenen Daten / anderen Auftragsdaten	☒	☐

Anlage

Organisationskontrolle	Bemerkung
Mitarbeiterschulung zum Datenschutz erfolgt?	Die nächste Schulung ist im Juni 2020 geplant.
Zutrittskontrolle	
Zutritt zum Gebäude beschränkt?	Türen sind per Codeschloss gesichert.
Erfolgt eine Besucherkontrolle?	Besucherkontrolle erfolgt durch Begleitung durch Mitarbeiter.
Besteht eine Videoüberwachung?	Sicherung relevanter Bereiche wie Büro und Serverräume durch Videoüberwachung.
Rechnerräume nur für befugtes Personal zugänglich?	Türen sind per Codeschloss gesichert.
Server sicher aufgestellt?	Serverräume sind nochmals separat mit eigenem Codesystem gesichert. Der Zugang ist nur befugten Mitarbeitern erlaubt. Die Zugänge werden protokolliert.
Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird (Akten, Datenträger)?	Türen sind per Codeschloss gesichert. Der Zugang ist nur befugten Mitarbeitern erlaubt.
Zugangskontrolle	
Benutzeridentifikation/Authentifizierung eingerichtet?	Jeder Mitarbeiter hat sich per Benutzername / Passwort zu authentifizieren.
Sichere Passwörter?	Es werden sichere Kennwörter nach festgelegten Kriterien verwendet.
Zugriffskontrolle	
Konzept für Zugriffsberechtigungen liegt vor?	Es existiert ein schriftliche Dokumentation der Berechtigungsvergabe. Need-to-know Prinzip wird umgesetzt.
Unterschiedliche Zugriffsrechte eingeteilt?	Vorhandenes Berechtigungskonzept nach Nutzgruppen/Mitarbeiter. Anzahl der Administratoren sind auf das „Notwendigste“ reduziert. Die Rechte werden durch Systemadministrator verwaltet.

	Unternehmensinterne Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel wird eingehalten.
Verletzungen werden protokoliert?	Bisher kam es zu keinen Verletzungen.
Kopierschutz/Bearbeitungsschutz eingerichtet?	Kundenbezogene Daten werden nur von befugten Mitarbeiter bearbeitet und eingesehen. Dies wird mit Zugriffsberechtigungen geregelt.

Weitergabekontrolle	
Beschränkung der Nutzung von privatem Equipment?	Das Unternehmen kauft die Endgeräte und stellt sie dem Arbeitnehmer zur Verfügung, sie bleiben jedoch Firmeneigentum. Der Arbeitgeber erlaubt dem Arbeitnehmer bei diesem Konzept die private Nutzung des Endgeräts unter seinen Bedingungen. Somit ist eine umfassende Kontrolle über das Endgerät und die darauf befindlichen Daten gewährleistet. Den Mitarbeitern stehen ein sicherer Zugang und eine verschlüsselte Datenübertragung in das Firmennetzwerk zur Verfügung. Die Daten werden nur konsumiert und nicht auf dem Endgerät gespeichert.

Eingabekontrolle	
Protokollierung von Verwaltungsakten?	Zu den Verwaltungsakten hat nur der Geschäftsführer Zugriff. Daher erfolgt keine Protokollierung.
Besteht eine schriftliche Dokumentation der Verfahren bei denen Daten des Auftraggebers verarbeitet werden?	Kundenbezogene Daten werden nur von befugten Mitarbeiter bearbeitet und eingesehen. Dies wird mit Zugriffsberechtigungen geregelt. Eine Schriftliche Dokumentation der Verfahren wurde bisher nicht durchgeführt.

Auftragskontrolle	
Bestehen Kontrollrechte des Auftraggebers beim Subunternehmer des Auftragnehmers?	Fa. rocom setzt keine Subunternehmen ein.
Konfliktmanagement bei Verstößen/Verdachtsfällen installiert?	Fa. rocom ist ein mittelständisches Unternehmen mit einem sehr guten Betriebsklima. Konfliktmanagement war bisher nicht notwendig.
Mechanismen zur Selbstkontrolle auf Seiten des Auftragnehmers vorhanden?	Die Selbstkontrolle erfolgt in Form des betrieblichen Datenschutzbeauftragten.

Trennungsgebot	
Besteht eine Trennung von Entwicklungs-, Test- und Produktivsystem?	Die Daten liegen auf unterschiedlichen Speicher- und Serversystemen.
Erfolgt eine Trennung der Daten des Auftraggebers von eigenen Daten / anderen Auftragsdaten	Die Trennung der Daten erfolgt im Rahmen des Berechtigungskonzepts.

Ort, Datum

Datenschutzbeauftragter

Geschäftsführer