

Anlage TOM

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

der Red Circle Productions GmbH

Unternehmen: Red Circle Productions GmbH

Anschrift: Parzellenstraße 28, 03050 Cottbus, Deutschland

Handelsregister: Amtsgericht Cottbus, HRB 15846 CB

Geschäftsführer: Floyd Block

Umsatzsteuer-Identifikationsnummer: DE350413132

Website: redcircle.de

Weitere Website / Marke: recruvoo.de

Datenschutzkontakt: datenschutz@redcircle.de

Hilfsweise Kontakt: media@redcircle.de

Stand: Mai 2026

0. Management Summary

Die Red Circle Productions GmbH hat ein angemessenes und dem Risiko entsprechendes Schutzniveau für personenbezogene Daten implementiert.

Die technischen und organisatorischen Maßnahmen orientieren sich am Stand der Technik, der Art, dem Umfang und den Zwecken der Verarbeitung sowie den Anforderungen der DSGVO, insbesondere Art. 32 DSGVO.

Die Maßnahmen berücksichtigen insbesondere die Verarbeitung personenbezogener Daten im Rahmen von:

- Social Recruiting,
- Recruvoo-Kampagnen,
- Leadgenerierung,
- Bewerbergewinnung,
- Social-Media-Kampagnen,
- Lead Ads,
- Lead Gen Forms,
- CRM-Prozessen,
- Landingpages,
- Bewerberformularen,
- Kontaktformularen,
- Content-Produktion,

- Kampagnenmanagement,
- Reporting,
- Kundenprojekten.

Die Maßnahmen werden mindestens einmal jährlich sowie anlassbezogen überprüft und bei Bedarf angepasst.

Die Maßnahmen werden regelmäßig evaluiert und entsprechen dem Stand der Technik unter Berücksichtigung der wirtschaftlichen Angemessenheit.

Verantwortlich für die Umsetzung, Überprüfung und Fortschreibung der TOM ist die Geschäftsführung der Red Circle Productions GmbH, vertreten durch den Geschäftsführer Floyd Block.

1. Zweck dieser Anlage

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen der Red Circle Productions GmbH zur Sicherheit der Verarbeitung personenbezogener Daten.

Die Maßnahmen dienen insbesondere dem Schutz personenbezogener Daten im Rahmen von:

- Social Recruiting,
- Recruvoo-Kampagnen,
- Bewerbergewinnung,
- Leadgenerierung,
- Auftragsgewinnung,
- Social-Media-Kampagnen,
- Lead Ads und Lead Gen Forms,
- Landingpages und Formularen,
- CRM-Prozessen,
- Reporting,
- Kundenprojekten,
- Website-, Funnel- und Trackingprozessen,
- Foto-, Video-, Content- und Kampagnenprojekten,
- Beratung, Schulungen, Workshops und digitalen Leistungen.

Diese Anlage ist Bestandteil des jeweiligen Vertrags über Auftragsverarbeitung, soweit Red Circle personenbezogene Daten im Auftrag eines Kunden verarbeitet.

2. Grundsatz der Angemessenheit

Red Circle trifft technische und organisatorische Maßnahmen, um personenbezogene Daten angemessen gegen Verlust, Missbrauch, unbefugten Zugriff, Veränderung, Offenlegung oder Zerstörung zu schützen.

Die Maßnahmen orientieren sich insbesondere an:

- Art, Umfang, Umständen und Zwecken der Verarbeitung,
- Eintrittswahrscheinlichkeit und Schwere möglicher Risiken,
- Art der verarbeiteten Daten,
- Zahl der betroffenen Personen,
- eingesetzten Systemen, Plattformen und Dienstleistern,
- technischen Möglichkeiten,
- wirtschaftlicher Angemessenheit,
- vereinbarten Leistungen,
- Weisungen des Auftraggebers,
- gesetzlichen Anforderungen.

Die konkreten Maßnahmen können je nach Projekt, Tool, Kampagne, Datenart und Auftrag variieren. Soweit besondere Risiken bestehen, können ergänzende Maßnahmen vereinbart werden.

Diese TOM enthalten keine pauschale Zusage zu bestimmten Zertifizierungen, Standards oder Rechenzentrumsbetrieben, insbesondere keine pauschale Zusage zu ISO-27001-Zertifizierungen, sofern diese nicht ausdrücklich gesondert vereinbart wurden oder durch einen eingesetzten Anbieter bereitgestellt werden.

Red Circle wählt Dienstleister, Tools und Plattformen mit angemessenem Sicherheits- und Datenschutzniveau aus und berücksichtigt dabei insbesondere Datenschutzinformationen, Sicherheitsinformationen, AV-Verträge, Anbieterangaben, Zugriffsmöglichkeiten, Lösch- und Exportfunktionen sowie die Eignung für den jeweiligen Projektzweck.

3. Geltungsbereich der Maßnahmen

Diese TOM gelten insbesondere für personenbezogene Daten, die Red Circle im Rahmen folgender Systeme oder Prozesse verarbeitet:

- Close.io bzw. Close CRM,
- OrgaMAX,
- Sharehub,
- Recruvoo-Systeme,

- eigene oder externe Dashboards,
- Webflow oder sonstige Website-/Landingpage-Systeme,
- E-Mail- und Kommunikationssysteme,
- Cloud- und Dateiverwaltungssysteme,
- Social-Media- und Werbeplattformen,
- Meta Business Suite,
- Google Ads,
- LinkedIn Ads,
- TikTok Ads,
- Formular- und Funnel-Systeme,
- Projektmanagementsysteme,
- Automationssysteme,
- Consent-Management-Systeme,
- KI-, Kreativ-, Analyse-, Foto-, Video- und Contenttools,
- sonstige im jeweiligen Projekt eingesetzte Software und Dienstleister.

Eine konkrete Übersicht der eingesetzten Dienstleister, Tools und Unterauftragnehmer ergibt sich aus der jeweils aktuellen Unterauftragnehmer- und Tool-Liste, der Leistungsbeschreibung, dem AVV sowie ergänzend aus der allgemeinen Datenschutzerklärung und deren Tool- bzw. Dienstleisterübersicht.

4. Vertraulichkeit

4.1 Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, unbefugten Personen den physischen Zugang zu Räumen, Geräten oder Unterlagen zu verwehren, in denen personenbezogene Daten verarbeitet werden.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein, soweit einschlägig:

- Nutzung geschlossener Geschäftsräume,
- kontrollierter Zugang zu Büroräumen,
- keine freie Zugänglichkeit vertraulicher Unterlagen für unbefugte Personen,
- Aufbewahrung vertraulicher Unterlagen an geschützten Orten,
- Zugriff auf Arbeitsgeräte nur durch berechtigte Personen,
- Sicherung mobiler Geräte gegen unbefugten Zugriff,
- sorgfältiger Umgang mit Besuchern, Dienstleistern und externen Personen,
- keine unbeaufsichtigte Offenlegung personenbezogener Daten in frei zugänglichen Bereichen.

Soweit Daten in Rechenzentren, Cloudsystemen oder SaaS-Diensten verarbeitet werden, liegt die physische Zutrittskontrolle beim jeweiligen Anbieter. Red Circle wählt solche Anbieter sorgfältig aus und berücksichtigt deren Sicherheits- und Datenschutzinformationen.

4.2 Zugangskontrolle

Ziel der Zugangskontrolle ist es, zu verhindern, dass unbefugte Personen IT-Systeme nutzen können, mit denen personenbezogene Daten verarbeitet werden.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Benutzerkonten nur für berechtigte Personen,
- individuelle Zugangsdaten und Passwortschutz,
- angemessene Passwortanforderungen,
- keine Weitergabe persönlicher Zugangsdaten,
- Sperrung oder Änderung von Zugängen bei Rollenwechsel, Projektende oder Ausscheiden,
- Zwei-Faktor-Authentifizierung, soweit verfügbar und angemessen,
- Zugriff auf CRM-, Projekt-, Ads-, Social-Media- und Cloudsysteme nur für berechtigte Personen,
- Gerätesperre bei Nichtbenutzung,
- Schutz mobiler Geräte durch PIN, Passwort, biometrische Sperre oder vergleichbare Maßnahmen,
- sichere Speicherung von Zugangsdaten,
- Einschränkung administrativer Rechte auf erforderliche Personen.

Soweit Plattformen eigene Sicherheitsfunktionen bereitstellen, insbesondere Rollen, Berechtigungen, Zwei-Faktor-Authentifizierung oder Aktivitätsprotokolle, werden diese nach Möglichkeit und Angemessenheit genutzt.

4.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, sicherzustellen, dass berechtigte Personen nur auf diejenigen personenbezogenen Daten zugreifen können, die sie für ihre jeweilige Aufgabe benötigen.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- rollen- und aufgabenbezogene Zugriffsrechte,
- Zugriff nach dem Need-to-know-Prinzip,

- getrennte Kundenbereiche oder Projektstrukturen, soweit technisch möglich und angemessen,
 - beschränkter Zugriff auf Bewerber-, Lead-, CRM- und Kundendaten,
 - beschränkter Zugriff auf Werbekonten, Dashboards und Reportingdaten,
 - regelmäßige Prüfung von Zugriffsrechten,
 - Entfernung nicht mehr benötigter Zugriffsrechte,
 - Vergabe von Administrationsrechten nur bei Erforderlichkeit,
 - Zugriff auf vertrauliche Projektunterlagen nur für Projektbeteiligte,
 - Zugriff auf AVV-, Vertrags-, Rechnungs- und Buchhaltungsdaten nur für berechtigte Personen.
-

4.4 Trennungskontrolle

Ziel der Trennungskontrolle ist es, personenbezogene Daten verschiedener Zwecke, Kunden oder Projekte angemessen getrennt zu verarbeiten.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- projektbezogene Ablage von Unterlagen und Daten,
 - getrennte Kundenbereiche oder Projektstrukturen, soweit technisch möglich,
 - getrennte CRM-Pipelines, Tags, Projekte oder Statusfelder, soweit erforderlich,
 - klare Zuordnung von Leads, Bewerbern und Kundenprojekten,
 - organisatorische Trennung zwischen eigenen Daten von Red Circle und im Auftrag verarbeiteten Kundendaten,
 - getrennte Behandlung von Interessenten-, Kunden-, Bewerber-, Lead-, Rechnungs- und Projektdaten,
 - Kennzeichnung projektbezogener Daten in CRM-, Projekt- oder Dateisystemen,
 - keine zweckfremde Nutzung von Kundendaten ohne geeignete Rechtsgrundlage oder Weisung.
-

4.5 Vertraulichkeitsverpflichtung

Red Circle stellt sicher, dass Personen, die personenbezogene Daten verarbeiten, zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind.

Hierzu gehören insbesondere:

- Vertraulichkeitsverpflichtungen für Mitarbeiter, freie Mitarbeiter und sonstige berechtigte Personen,
- Sensibilisierung für den vertraulichen Umgang mit personenbezogenen Daten,
- Verbot unbefugter Weitergabe personenbezogener Daten,

- Verpflichtung zur Einhaltung von Weisungen und internen Datenschutzregeln,
 - Schutz vertraulicher Kunden-, Bewerber-, Lead- und Projektdaten,
 - besondere Sensibilität bei Bewerberdaten, Recruitingdaten, CRM-Daten und Kampagnendaten.
-

5. Integrität

5.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu verhindern, dass personenbezogene Daten bei Übertragung, Transport oder Speicherung unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Übermittlung personenbezogener Daten nur an berechtigte Empfänger,
- Weitergabe von Bewerber- oder Lead-Daten an Kunden nur im Rahmen des jeweiligen Auftrags,
- Nutzung sicherer Kommunikationswege, soweit angemessen,
- verschlüsselte Übertragung bei webbasierten Diensten, soweit verfügbar,
- Vermeidung unnötiger Datenanhänge per E-Mail,
- sorgfältige Prüfung von Empfängern vor Datenweitergabe,
- Zugriffsbeschränkung bei Cloudfreigaben,
- zeitliche oder projektbezogene Beschränkung von Freigaben, soweit möglich,
- keine Veröffentlichung personenbezogener Daten ohne geeignete Rechtsgrundlage, Freigabe oder Einwilligung,
- Beachtung von Kundenweisungen bei Datenübermittlungen.

Bei der Weitergabe an Auftraggeber, Kunden, Plattformen oder Dienstleister wird jeweils geprüft, ob Red Circle als Verantwortlicher, Auftragsverarbeiter, gemeinsam Verantwortlicher oder rein unterstützender Dienstleister handelt.

5.2 Eingabekontrolle

Ziel der Eingabekontrolle ist es, nachvollziehen zu können, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden, soweit dies technisch möglich und angemessen ist.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Nutzung systemseitiger Protokollierungen, soweit durch die eingesetzten Tools verfügbar,

- Dokumentation wesentlicher Bearbeitungsschritte in CRM- oder Projektmanagementsystemen,
 - Nachvollziehbarkeit von Lead-, Bewerber- oder Projektstatus, soweit systemseitig möglich,
 - Nutzung von Zeitstempeln, Benutzerhistorien oder Aktivitätsprotokollen, soweit verfügbar,
 - Dokumentation wichtiger Freigaben, Weisungen und Kundenentscheidungen,
 - nachvollziehbare Bearbeitung von Kampagnen, Formularen, Bewerberdaten und Lead-Daten,
 - Einschränkung von Schreib- und Änderungsrechten auf berechnigte Personen.
-

5.3 Datenrichtigkeit und Aktualität

Red Circle trifft angemessene Maßnahmen, um personenbezogene Daten im Rahmen der jeweiligen Verarbeitung sachlich richtig und aktuell zu halten, soweit dies erforderlich und möglich ist.

Hierzu gehören insbesondere:

- Korrektur fehlerhafter Daten nach Kenntnis,
 - Aktualisierung von Lead-, Bewerber-, Kunden- und Projektdaten bei relevanten Änderungen,
 - Berücksichtigung von Korrekturwünschen betroffener Personen,
 - Weiterleitung von Berichtigungsanfragen an Auftraggeber, soweit Red Circle als Auftragsverarbeiter tätig ist,
 - Vermeidung unnötiger Dubletten, soweit möglich,
 - regelmäßige Prüfung projektbezogener Datenbestände nach Erforderlichkeit.
-

6. Verfügbarkeit und Belastbarkeit

6.1 Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen und die Verfügbarkeit der Systeme angemessen sicherzustellen.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Nutzung professioneller Cloud-, SaaS-, CRM-, Hosting- und Plattformanbieter,
- Auswahl von Dienstleistern mit angemessenen Sicherheits- und Verfügbarkeitsmaßnahmen,
- Nutzung systemseitiger Backup-, Versionierungs- und Wiederherstellungsfunktionen, soweit angeboten,

- Schutz von Arbeitsgeräten gegen unbefugten Zugriff,
 - angemessene Gerätesicherheit,
 - Schutz wichtiger Zugangsdaten,
 - Einsatz aktueller Softwareversionen, soweit möglich und angemessen,
 - strukturierte Ablage wichtiger Projekt-, Kunden- und Vertragsdaten,
 - Wiederherstellungsmöglichkeiten über eingesetzte Anbieter, soweit verfügbar,
 - Berücksichtigung von Verfügbarkeit und Wiederherstellbarkeit bei der Auswahl relevanter Tools.
-

6.2 Backup und Wiederherstellung

Red Circle nutzt je nach System und Verarbeitung die systemseitigen Backup-, Versionierungs- und Wiederherstellungsfunktionen der eingesetzten professionellen Cloud-, Hosting-, CRM- und SaaS-Anbieter.

Dies betrifft insbesondere eingesetzte Systeme wie CRM-, Website-, Landingpage-, Projekt-, Datei-, Kommunikations-, Hosting- und Cloudsysteme, soweit die jeweiligen Anbieter entsprechende Funktionen bereitstellen.

Maßnahmen können insbesondere sein:

- regelmäßige systemseitige Backups durch eingesetzte Cloud-, Hosting-, CRM- oder SaaS-Anbieter, soweit vom Anbieter bereitgestellt,
- Nutzung von Versionierungs- und Wiederherstellungsfunktionen in Dokumenten-, Projekt- oder Cloudsystemen, soweit verfügbar,
- zusätzliche Sicherung oder Export wichtiger Projekt-, Vertrags-, Kampagnen- oder Kundendaten nach Erforderlichkeit,
- Schutz wichtiger Dokumente vor unbeabsichtigtem Verlust,
- Wiederherstellung gelöschter oder geänderter Daten, soweit technisch möglich,
- anlassbezogene Prüfung der Wiederherstellbarkeit, insbesondere bei Toolwechseln, größeren Projekten oder sicherheitsrelevanten Änderungen,
- regelmäßige Überprüfung der Backup- und Wiederherstellungsfunktionalität, soweit dies Red Circle technisch möglich ist und nicht ausschließlich im Verantwortungsbereich des jeweiligen Anbieters liegt.

Die konkrete Backup- und Wiederherstellungslogik hängt vom jeweils eingesetzten System, Anbieter und Projektsetup ab.

Soweit Backups durch Drittanbieter erfolgen, gelten zusätzlich die Regelungen des jeweiligen Anbieters. Red Circle prüft die Verfügbarkeit und Funktionsfähigkeit der Backups anlassbezogen, soweit dies technisch möglich ist und nicht ausschließlich im Verantwortungsbereich des jeweiligen Anbieters liegt.

6.3 Belastbarkeit der Systeme

Red Circle setzt überwiegend professionelle Drittanbieter-, Plattform-, Cloud- und SaaS-Systeme ein. Die technische Belastbarkeit dieser Systeme richtet sich insbesondere nach den Sicherheits-, Verfügbarkeits- und Infrastrukturmaßnahmen der jeweiligen Anbieter.

Red Circle berücksichtigt bei der Auswahl und Nutzung solcher Anbieter insbesondere:

- geschäftliche Eignung,
- Sicherheitsinformationen,
- Datenschutzinformationen,
- AV-Verträge oder vergleichbare Datenschutzregelungen, soweit erforderlich,
- Zugriffsmöglichkeiten,
- Benutzer- und Rechteverwaltung,
- Export- oder Löschmöglichkeiten,
- technische Stabilität,
- Verfügbarkeit im üblichen Geschäftsbetrieb.

Bei Plattformen wie Meta, Google, LinkedIn, TikTok oder vergleichbaren Werbe- und Social-Media-Plattformen bestimmt der jeweilige Plattformanbieter wesentliche technische Schutzmaßnahmen, Verfügbarkeiten, Protokolle, Schnittstellen und Sicherheitsfunktionen eigenständig.

7. Pseudonymisierung, Datenminimierung und Verschlüsselung

7.1 Datenminimierung

Red Circle verarbeitet personenbezogene Daten nur, soweit dies für den jeweiligen Zweck erforderlich ist.

Maßnahmen zur Datenminimierung sind insbesondere:

- Erhebung nur erforderlicher Formularfelder,
- Vermeidung unnötiger Pflichtfelder,
- projektbezogene Festlegung erforderlicher Daten,
- keine aktive Abfrage besonderer Kategorien personenbezogener Daten, soweit nicht erforderlich,
- Reduzierung personenbezogener Daten in Reports, soweit möglich,
- Nutzung aggregierter oder anonymisierter Kampagnendaten, soweit ausreichend,
- keine unnötige Speicherung von Bewerber- oder Lead-Daten,

- Löschung oder Archivierung nach Zweckerreichung, soweit keine Aufbewahrungsgründe bestehen.
-

7.2 Pseudonymisierung und Anonymisierung

Red Circle setzt Pseudonymisierung oder Anonymisierung ein, soweit dies für den jeweiligen Zweck möglich und angemessen ist.

Dies betrifft insbesondere:

- Kampagnenauswertungen,
- Performance-Reports,
- interne Analysen,
- Fallbeispiele,
- Referenzen,
- KI-gestützte Arbeitsprozesse,
- Testdaten,
- Schulungs- und Beratungsunterlagen.

Beispiele:

- In Reportings werden nach Möglichkeit aggregierte Kennzahlen statt einzelner Namen verwendet.
- Bei Kampagnenanalysen können Lead- oder Bewerberdaten auf Kampagnenquelle, Status, Zeitraum oder Qualifikationsgruppe reduziert werden.
- Bei internen Beispielen, Schulungen oder KI-gestützten Arbeitsprozessen können Namen, Telefonnummern, E-Mail-Adressen, Unternehmensdetails oder sonstige direkte Identifikatoren entfernt, gekürzt oder ersetzt werden.
- Bei Case Studies werden personenbezogene Daten nach Möglichkeit anonymisiert, aggregiert oder nur nach Freigabe verwendet.

Soweit personenbezogene Daten für den jeweiligen Zweck nicht erforderlich sind, werden Daten möglichst anonymisiert, aggregiert oder auf ein erforderliches Minimum reduziert.

7.3 Verschlüsselung

Red Circle nutzt Verschlüsselung, soweit diese technisch verfügbar, angemessen und durch die jeweiligen Systeme oder Anbieter unterstützt wird.

Maßnahmen können insbesondere sein:

- HTTPS-/TLS-verschlüsselte Verbindungen bei Websites, Formularen, Landingpages und Cloud-Diensten,

- bevorzugte Nutzung moderner Transportverschlüsselung, insbesondere TLS 1.2 oder höher, soweit durch Anbieter, Browser und System unterstützt,
- bevorzugte Nutzung von TLS 1.3, soweit verfügbar,
- Transportverschlüsselung durch eingesetzte SaaS-, Cloud- und Plattformanbieter,
- Passwortschutz für Systeme, Accounts und Geräte,
- Geräteverschlüsselung bei Endgeräten, soweit verfügbar, angemessen und aktiviert,
- Verschlüsselung ruhender Daten bei Cloud-, Hosting-, CRM- oder SaaS-Anbietern, soweit vom jeweiligen Anbieter unterstützt und aktiviert,
- sichere Speicherung von Zugangsdaten,
- Nutzung von Verschlüsselungs- und Sicherheitsfunktionen der eingesetzten Anbieter,
- verschlüsselte Kommunikation oder geschützte Freigaben, soweit im konkreten Fall erforderlich und verfügbar.

Die konkrete Verschlüsselung hängt vom jeweiligen System, Anbieter, Kommunikationsweg und Projektsetup ab.

8. Auftragskontrolle

Ziel der Auftragskontrolle ist es, sicherzustellen, dass personenbezogene Daten, die Red Circle im Auftrag eines Kunden verarbeitet, nur entsprechend dem Vertrag und den dokumentierten Weisungen des Kunden verarbeitet werden.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Abschluss eines AV-Vertrags, soweit Red Circle als Auftragsverarbeiter tätig ist,
- Verarbeitung personenbezogener Daten nur im Rahmen des vereinbarten Auftrags,
- Beachtung dokumentierter Weisungen des Auftraggebers,
- Beschreibung der Verarbeitung in Leistungsbeschreibung, Angebot, AVV oder Anlage,
- Festlegung von Zweck, Datenarten, Betroffenenengruppen und Verarbeitungsvorgängen,
- Weitergabe von Bewerber- oder Lead-Daten an den jeweiligen Auftraggeber nur im Rahmen des Auftrags,
- keine eigenmächtige Zweckänderung von Auftragsdaten,
- Unterstützung des Auftraggebers bei Betroffenenanfragen, soweit gesetzlich und vertraglich vorgesehen,
- Unterstützung bei Löschung, Rückgabe oder Export von Daten nach Auftragsende, soweit vereinbart,
- Einbindung von Unterauftragnehmern nur nach Maßgabe des AVV.

Soweit Red Circle nicht als Auftragsverarbeiter, sondern als eigener Verantwortlicher oder gemeinsam Verantwortlicher tätig wird, gelten die hierfür einschlägigen Datenschutzinformationen, Vereinbarungen und gesetzlichen Regelungen.

9. Unterauftragnehmer und Dienstleister

Red Circle kann zur Leistungserbringung Unterauftragnehmer, Plattformen, SaaS-Anbieter, Freelancer, technische Dienstleister oder sonstige Dienstleister einsetzen.

Hierzu können je nach Projekt insbesondere gehören:

- Hostinganbieter,
- Website- und Landingpage-Systeme,
- CRM-Anbieter,
- Projektmanagementsysteme,
- E-Mail- und Kommunikationsdienste,
- Social-Media- und Werbeplattformen,
- Tracking- und Analyseanbieter,
- Consent-Management-Anbieter,
- Zahlungs- und Buchhaltungsanbieter,
- KI-, Kreativ-, Foto-, Video- und Audiotools,
- Freelancer und spezialisierte Projektpartner.

Red Circle achtet bei der Auswahl solcher Dienstleister auf eine angemessene Eignung und berücksichtigt Datenschutz- und Sicherheitsanforderungen.

Soweit ein Dienstleister als Unterauftragnehmer im Sinne der Auftragsverarbeitung eingesetzt wird, erfolgt die Einbindung nach Maßgabe des jeweiligen AVV.

Eine konkrete Übersicht der eingesetzten Unterauftragnehmer und Tools ergibt sich aus der jeweils aktuellen Unterauftragnehmer- und Tool-Liste. Ergänzend können Angaben in der allgemeinen Datenschutzerklärung und deren Tool- bzw. Dienstleisterübersicht enthalten sein.

10. Löschung, Rückgabe und Einschränkung der Verarbeitung

Red Circle löscht, exportiert, übergibt oder beschränkt personenbezogene Daten nach Maßgabe des jeweiligen Vertrags, AVV, der dokumentierten Weisungen des Auftraggebers und gesetzlicher Vorgaben.

Maßnahmen können insbesondere sein:

- Löschung nicht mehr erforderlicher Lead- oder Bewerberdaten,
- Export oder Übergabe von Daten an den Auftraggeber,
- Einschränkung der weiteren Verarbeitung nach Projektende,
- Beachtung gesetzlicher Aufbewahrungsfristen,
- Beachtung berechtigter Nachweis- und Verteidigungsinteressen,
- Löschung oder Anonymisierung von Testdaten,
- Entfernung nicht mehr benötigter Zugriffsrechte,
- Berücksichtigung von Backup-, Archiv- und Protokollfristen der eingesetzten Systeme.

Soweit Red Circle als Auftragsverarbeiter tätig ist, richtet sich die Löschung, Rückgabe oder weitere Speicherung nach dem AVV und den Weisungen des Auftraggebers.

11. Rechte betroffener Personen

Red Circle unterstützt den Auftraggeber nach Maßgabe des AVV und der gesetzlichen Vorgaben bei der Bearbeitung von Anfragen betroffener Personen.

Dies betrifft insbesondere Anfragen zu:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenübertragbarkeit,
- Widerspruch,
- Widerruf von Einwilligungen,
- Beschwerden oder sonstigen Datenschutzanliegen.

Soweit Red Circle eine Anfrage erhält, die Daten betrifft, die im Auftrag eines Kunden verarbeitet werden, kann Red Circle die Anfrage an den Auftraggeber weiterleiten oder nach dessen Weisung bearbeiten.

12. Datenschutzvorfälle und Meldewege

Red Circle trifft angemessene organisatorische Maßnahmen, um Datenschutzvorfälle zu erkennen, zu bewerten und zu bearbeiten.

Maßnahmen können insbesondere sein:

- interne Meldewege für Datenschutz- und Sicherheitsvorfälle,
- Prüfung des betroffenen Systems oder Vorgangs,
- Bewertung möglicher Auswirkungen,
- Dokumentation relevanter Informationen,
- Information des Auftraggebers bei Auftragsverarbeitung nach Maßgabe des AVV,
- Mitwirkung bei erforderlichen Folgemaßnahmen,
- Unterstützung bei gesetzlichen Melde- und Informationspflichten, soweit vereinbart und erforderlich,
- Maßnahmen zur Eindämmung und Vermeidung weiterer Schäden.

Datenschutzvorfälle können insbesondere sein:

- unbefugter Zugriff,
- versehentliche Offenlegung,
- Verlust von Geräten oder Unterlagen,
- Fehlversand von personenbezogenen Daten,
- unberechtigte Datenweitergabe,
- Kompromittierung von Zugangsdaten,
- Sicherheitsvorfälle bei eingesetzten Dienstleistern.

Soweit ein Datenschutzvorfall Systeme oder Daten eines Plattform-, Cloud-, SaaS- oder Dienstleistungsanbieters betrifft, hängt die Aufklärung auch von den Informationen und Mitwirkungsmöglichkeiten des jeweiligen Anbieters ab.

13. Prüfung, Bewertung und Evaluierung

Red Circle überprüft und bewertet die Angemessenheit der technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen.

Eine Überprüfung erfolgt insbesondere:

- bei Einführung neuer Tools,
- bei neuen Kundenprojekten mit besonderen Risiken,
- bei neuen Verarbeitungsvorgängen,
- bei Änderungen in Kampagnenprozessen,
- bei Änderungen bei Plattformen oder Dienstleistern,
- bei Datenschutzvorfällen,
- bei neuen rechtlichen Anforderungen,
- bei wesentlichen technischen oder organisatorischen Änderungen.

Maßnahmen können insbesondere sein:

- Prüfung eingesetzter Tools und Zugriffsrechte,
- Aktualisierung der Unterauftragnehmer- und Tool-Liste,
- Anpassung von Rollen und Berechtigungen,
- Prüfung von Datenschutzinformationen und AV-Verträgen,
- Anpassung von Lösch- und Aufbewahrungsprozessen,
- Anpassung von Formular-, Consent- und Kampagnenprozessen,
- Aktualisierung interner Hinweise und Vorlagen.

Die TOM werden mindestens einmal jährlich sowie anlassbezogen überprüft und bei Bedarf fortgeschrieben.

Eine anlassbezogene Prüfung erfolgt insbesondere bei:

- wesentlichen Änderungen der Verarbeitung,
- Einführung neuer Tools,
- Einführung neuer Plattformen,
- neuen Risiken,
- neuen Kundenprojekten mit besonderem Schutzbedarf,
- Änderungen bei Unterauftragnehmern,
- Änderungen der eingesetzten Cloud-, CRM-, Ads-, Tracking-, KI- oder Plattformdienste,
- relevanten Datenschutzvorfällen,
- neuen rechtlichen oder technischen Anforderungen.

Die Prüfung kann insbesondere die Aktualität der Tool- und Unterauftragnehmerliste, die Zugriffsrechte, die Lösch- und Backup-Prozesse, die Consent- und Tracking-Konfigurationen, die KI-Nutzung sowie die Dokumentation von Weisungen und Freigaben betreffen.

Die Ergebnisse der Überprüfungen werden in angemessener Form dokumentiert.

14. Schulung und Sensibilisierung

Red Circle sensibilisiert berechtigte Personen für den Umgang mit personenbezogenen Daten.

Dies umfasst insbesondere:

- vertraulichen Umgang mit Kundendaten,
- vertraulichen Umgang mit Bewerber- und Lead-Daten,
- sichere Nutzung von CRM-, Ads-, Projekt- und Cloudsystemen,

- Schutz von Zugangsdaten,
 - Umgang mit Phishing- und Sicherheitsrisiken,
 - besondere Vorsicht bei sensiblen Daten,
 - Beachtung von Lösch- und Aufbewahrungsvorgaben,
 - Beachtung von Kundenweisungen,
 - Datenschutz bei KI-, Kreativ- und Contenttools.
-

15. Homeoffice, mobiles Arbeiten und externe Arbeit

Soweit Mitarbeiter, Freelancer oder berechnigte Personen mobil oder außerhalb der Geschäftsräume arbeiten, gelten angemessene Schutzmaßnahmen.

Dazu können insbesondere gehören:

- Nutzung geschützter Geräte,
 - Zugriff nur durch berechnigte Personen,
 - Gerätesperre bei Nichtbenutzung,
 - Schutz von Zugangsdaten,
 - keine unbefugte Einsichtnahme durch Dritte,
 - vertrauliche Gespräche nicht in ungeeigneten Umgebungen,
 - sorgfältiger Umgang mit Ausdrucken oder Notizen,
 - Nutzung sicherer Netzwerkverbindungen, soweit möglich,
 - keine Speicherung personenbezogener Daten auf privaten oder ungeschützten Speichermedien, soweit vermeidbar,
 - Löschung nicht mehr benötigter lokaler Kopien.
-

16. KI-, Kreativ- und Automationssysteme

Red Circle kann KI-, Kreativ-, Analyse-, Automations-, Text-, Bild-, Video- oder Audiotools einsetzen, soweit dies für den jeweiligen Zweck erforderlich oder zweckmäßig ist.

Zum Schutz personenbezogener Daten gelten insbesondere folgende Maßnahmen:

- Nutzung personenbezogener Daten in KI-Tools nur, soweit hierfür eine geeignete Grundlage besteht,
- Reduzierung personenbezogener Daten auf das erforderliche Maß,
- bevorzugte Nutzung anonymisierter, pseudonymisierter oder gekürzter Informationen,

- keine Eingabe sensibler, vertraulicher oder besonders schutzbedürftiger Daten in KI-Tools ohne geeignete Rechtsgrundlage, Weisung, Einwilligung oder vertragliche Grundlage,
- Beachtung von Kundenweisungen bei KI-Nutzung im Auftrag,
- Prüfung geeigneter Anbieterinformationen und Einstellungen, soweit verfügbar,
- keine Nutzung von KI-Ergebnissen als alleinige Grundlage für rechtlich erhebliche Entscheidungen,
- angemessene Prüfung KI-gestützter Arbeitsergebnisse im Rahmen des jeweiligen Leistungsumfangs.

Soweit KI-Tools, Kreativtools oder Plattformdienste personenbezogene Daten für eigene Zwecke verarbeiten oder eigenständig über wesentliche technische Mittel entscheiden, richtet sich deren Verantwortung nach den jeweiligen Anbieterbedingungen, Datenschutzinformationen und vertraglichen Regelungen.

Red Circle übernimmt keine Verantwortung für eigenständige Datenverarbeitungen solcher Anbieter, soweit Red Circle diese Verarbeitung nicht selbst veranlasst oder rechtlich mitverantwortet.

17. Social-Media-, Ads- und Plattformzugriffe

Bei der Nutzung von Social-Media-, Ads-, Tracking- und Plattformkonten gelten besondere Schutzmaßnahmen.

Dazu können insbesondere gehören:

- Zugriff auf Werbekonten nur für berechtigte Personen,
- Zugriff auf Kundenaccounts nur nach Freigabe oder Einladung,
- rollenbasierte Berechtigungen, soweit durch die Plattform möglich,
- Entfernung von Zugängen nach Projektende oder bei Rollenwechsel,
- keine Weitergabe persönlicher Plattformzugänge,
- Nutzung von Zwei-Faktor-Authentifizierung, soweit verfügbar und angemessen,
- sorgfältige Verwaltung von Business Manager-, Ads-, Analytics- und Trackingzugängen,
- Prüfung von Kampagnenfreigaben,
- Trennung von Kundenprojekten und eigenen Kampagnen, soweit möglich,
- Dokumentation wesentlicher Freigaben und Weisungen.

Plattformanbieter wie Meta, Google, LinkedIn, TikTok oder vergleichbare Anbieter bestimmen viele Sicherheits-, Rollen-, Protokollierungs-, Export-, Lösch- und Zugriffsfunktionen eigenständig. Red Circle nutzt solche Funktionen im Rahmen der verfügbaren Möglichkeiten und des jeweiligen Projektsetups.

18. Formular-, Landingpage- und Trackingprozesse

Bei Formularen, Landingpages, Bewerberformularen, Recruvoo-Prozessen und Lead-Kampagnen achtet Red Circle insbesondere auf:

- Einbindung geeigneter Datenschutzhinweise,
 - Verlinkung der Datenschutzerklärung und Spezial-Datenschutzhinweise,
 - Einbindung eines Impressums oder Anbieterhinweises, soweit erforderlich,
 - Datenminimierung bei Formularfeldern,
 - klare Zweckbestimmung,
 - transparente Information bei Weitergabe an Auftraggeber,
 - Einwilligungen für Talentpool, Newsletter oder Marketing, soweit erforderlich,
 - Consent-Banner oder vergleichbare Einwilligungslösung für nicht notwendige Cookies, Pixel oder Tracking-Technologien, soweit erforderlich,
 - Prüfung der technischen Einbindung von Pixeln, Tags und Conversion APIs,
 - keine unnötige Erhebung besonderer Kategorien personenbezogener Daten.
-

19. Foto-, Video-, Audio- und Contentproduktionen

Bei Foto-, Video-, Audio-, Event-, Studio-, Creator-, UGC- oder Contentproduktionen können personenbezogene Daten in Bild, Ton, Text oder sonstigen Inhalten verarbeitet werden.

Red Circle setzt hierzu insbesondere folgende Maßnahmen ein:

- Einholung erforderlicher Einwilligungen oder vertraglicher Freigaben, soweit erforderlich,
 - Nutzung von Model Releases oder vergleichbaren Freigaben bei werblicher Nutzung erkennbarer Personen,
 - Prüfung von Nutzungsrechten und Veröffentlichungsrechten,
 - beschränkter Zugriff auf Rohmaterial und Projektdateien,
 - projektbezogene Ablage von Medienmaterial,
 - keine Veröffentlichung personenbezogener Inhalte ohne geeignete Grundlage,
 - besondere Vorsicht bei Mitarbeitern, Bewerbern, Verbrauchern, Kindern oder sonstigen schutzbedürftigen Personen,
 - Löschung oder Archivierung nach Zweck, Vereinbarung, Rechtsgrundlage und Aufbewahrungsbedarf.
-

20. Referenzen, Case Studies und Projektergebnisse

Bei Referenzen, Case Studies, Testimonials, Kampagnenergebnissen, Screenshots, Logos oder Projektbeispielen achtet Red Circle darauf, personenbezogene Daten nur zu verwenden, soweit dies zulässig ist.

Maßnahmen können insbesondere sein:

- Nutzung anonymisierter oder aggregierter Kennzahlen, soweit ausreichend,
 - Einholung von Freigaben, soweit erforderlich,
 - Vermeidung unnötiger personenbezogener Details,
 - Prüfung von Bild-, Namens-, Marken- und Nutzungsrechten,
 - Beschränkung personenbezogener Informationen auf das erforderliche Maß,
 - Beachtung berechtigter Einwände betroffener Personen.
-

21. Dokumentation und Nachweisbarkeit

Red Circle dokumentiert wesentliche Datenschutz- und Sicherheitsmaßnahmen in angemessener Form.

Hierzu können insbesondere gehören:

- AV-Verträge,
- TOM-Anlagen,
- Unterauftragnehmer- und Tool-Listen,
- Leistungsbeschreibungen,
- Kundenweisungen,
- Freigaben,
- Consent- und Formularnachweise,
- interne Datenschutz- und Sicherheitsnotizen,
- Lösch- und Exportnachweise, soweit erforderlich,
- Dokumentation von Datenschutzvorfällen,
- Versionierung relevanter Datenschutzdokumente.

Die konkrete Dokumentation richtet sich nach Art, Umfang, Risiko und Zweck der jeweiligen Verarbeitung.

22. Stand der Maßnahmen und Änderungen

Diese TOM beschreiben die zum Stand dieser Anlage allgemein vorgesehenen technischen und organisatorischen Maßnahmen von Red Circle.

Red Circle kann Maßnahmen anpassen, ersetzen oder weiterentwickeln, wenn:

- sich eingesetzte Tools ändern,
- neue technische Möglichkeiten entstehen,
- neue rechtliche Anforderungen relevant werden,
- Kundenprojekte besondere Anforderungen stellen,
- Sicherheits- oder Datenschutzrisiken dies erfordern,
- Dienstleister oder Plattformen ihre Systeme ändern,
- betriebliche Abläufe angepasst werden.

Änderungen dürfen das vereinbarte Schutzniveau nicht unangemessen unterschreiten.

23. Besondere Zusatzmaßnahmen nach Projektbedarf

Je nach Auftrag, Datenart, Risiko oder Kundenanforderung können ergänzende Maßnahmen vereinbart werden.

Solche Zusatzmaßnahmen können insbesondere betreffen:

- strengere Zugriffsbeschränkungen,
- besondere Löschfristen,
- gesonderte Exportprozesse,
- besondere Freigabeprozesse,
- besondere Verschlüsselung,
- gesonderte Kundensysteme,
- zusätzliche Vertraulichkeitsvereinbarungen,
- gesonderte KI-Beschränkungen,
- Ausschluss bestimmter Tools,
- besondere Reportingvorgaben,
- besondere Dokumentation von Weisungen,
- besondere Fristen bei Datenschutzvorfällen.

Solche Zusatzmaßnahmen bedürfen einer gesonderten Vereinbarung oder dokumentierten Weisung.

24. Versionshistorie

Version	Stand	Änderung
1.0	Mai 2026	Ergänzung zur wirtschaftlichen Angemessenheit, Klarstellung zur Backup-Prüfung, Dokumentation der Überprüfungsergebnisse und finale redaktionelle Straffung

25. Zusammenfassung der Schutzbereiche

Die technischen und organisatorischen Maßnahmen von Red Circle umfassen insbesondere:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Belastbarkeit,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Trennungskontrolle,
- Auftragskontrolle,
- Datenminimierung,
- Pseudonymisierung und Anonymisierung,
- Verschlüsselung, soweit angemessen,
- Backup- und Wiederherstellungsmaßnahmen,
- Lösch- und Rückgabeverfahren,
- Datenschutzvorfallmanagement,
- Dienstleister- und Unterauftragnehmerkontrolle,
- Schulung und Sensibilisierung,
- Prüfung und Weiterentwicklung der Maßnahmen,
- Dokumentation und Nachweisbarkeit.

Schutzziel	Umsetzung	Verantwortung
Vertraulichkeit	Zutritts-, Zugangs-, Zugriffskontrolle und Vertraulichkeitsverpflichtungen	Red Circle und eingesetzte Anbieter
Integrität	Weitergabekontrolle, Eingabekontrolle, Trennungskontrolle und Berechtigungskonzepte	Red Circle
Verfügbarkeit	Professionelle Cloud-, Hosting-, CRM- und SaaS-Anbieter sowie Backup- und Wiederherstellungsfunktionen	Anbieter und Red Circle
Belastbarkeit	Auswahl geeigneter Plattformen, Systeme und Anbieter mit angemessenem Sicherheitsniveau	Anbieter und Red Circle
Auftragskontrolle	AV-Verträge, Leistungsbeschreibungen, Weisungsbindung und Unterauftragnehmerkontrollen	Red Circle und Auftraggeber
Datenschutzvorfälle	Interne Meldewege, Bewertung, Dokumentation und Information nach Maßgabe des AVV	Red Circle
Datenminimierung	Reduzierung von Formularfeldern, Reports, KI-Eingaben und Projektinformationen auf das erforderliche Maß	Red Circle
Pseudonymisierung / Anonymisierung	Aggregierte Reports, gekürzte Beispiele, anonymisierte Case Studies und reduzierte Testdaten	Red Circle
Verschlüsselung	HTTPS/TLS, Passwortschutz, geschützte Freigaben und Anbieter-Verschlüsselung, soweit verfügbar	Anbieter und Red Circle

Schutzziel	Umsetzung	Verantwortung
Regelmäßige Prüfung	Mindestens jährliche und anlassbezogene Überprüfung der TOM	Red Circle

Ende der Anlage TOM – Technische und organisatorische Maßnahmen der Red Circle Productions GmbH – Stand Mai 2026