**Anlage**

# **Auftragsverarbeitungsvereinbarung** nach Art. 28 EU-Datenschutzgrundverordnung (DSGVO)

Version 1.5 vom 15.08.2023

Zwischen der:

- nachstehend „**Auftraggeber**“ genannt –

und der:

**Inxmail GmbH**
Wentzingerstraße 17
79106 Freiburg
Deutschland

- nachstehend „**Inxmail**“ genannt –

# 1 Vorbemerkungen

Inxmail ist Hersteller der Software „Inxmail Professional“, „Inxmail Commerce“ und „Inxmail Advertate“ (im Folgenden: „**Software**“), die als Internet-Dienst (Software-as-a-Service; ASP-Service) angeboten wird (dann im Folgenden als „**Service**“ bezeichnet). Mit dem Service können Nutzer – jeweils an eine E-Mail-Adresse anknüpfend – Daten sowie personenbezogene Daten pflegen, nutzen und auswerten.

Die Services werden auf Grundlage des zwischen den Parteien geschlossenen Vertrags über die Nutzung von Software als ASP Service (im Folgenden „**Hauptvertrag**“) erbracht.

Diese Vereinbarung regelt den Umgang mit personenbezogenen Daten im Rahmen der Services. Sofern weitere Dienstleistungen (wie z. B. Training- oder Consultingdienstleistungen) bei Inxmail zum bestehenden Hauptvertrag durch den Auftraggeber hinzugebucht / bestellt werden, unterliegen diese ebenfalls der in diesem Dokument getroffenen Auftragsverarbeitungsvereinbarung.

# 2 Gegenstand der Vereinbarung

## 2.1 Gegenstand und Dauer des Auftrages:

Inxmail verarbeitet im Rahmen des Hostings der Software personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand des Auftrages und genaue Umfang der Datenverarbeitung ergibt sich aus dem aktuell gültigen Hauptvertrag sowie aus etwaigen Einzelweisungen.

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

## 2.2 Art und Zweck der Datenverarbeitung:

Der Umfang und Zweck der Tätigkeit von Inxmail für den Auftraggeber ergibt sich aus dem Hauptvertrag sowie aus etwaigen Einzelweisungen.

Im Rahmen des Auftragsverhältnisses mit dem Auftraggeber verarbeitet Inxmail dabei ausschließlich personenbezogene Daten, welche auf Veranlassung des Auftraggebers oder vom Auftraggeber selbst in den jeweiligen Service eingestellt werden. Inxmail wird diese Daten in keinem Fall ohne ausdrückliche Weisung des Auftraggebers in einem weiteren Umfang oder für einen weitergehenden Zweck verarbeiten.

## 2.3 Datenarten und Kreis der betroffenen Personen:

Die Art und Menge der vom Service genutzten personenbezogenen Daten und betroffenen Personengruppen hängt vom Einsatz der Software durch den Auftraggeber ab. Regelmäßig sind dies vor allem E-Mail-Adresse, Anrede, Titel, Vorname, Nachname und Nutzerverhalten von Kunden, Interessenten und/oder Mitarbeitern. Inxmail wird in keinem Fall ohne ausdrückliche Weisung des Auftraggebers weitergehende Arten von Daten oder betroffenen Personen verarbeiten.

Von der Verarbeitung in Inxmail Software und Services ausgeschlossen sind besondere Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 DSGVO.

Eine Spezifikation der Art der Daten und Kategorien der Betroffenen erfolgt sofern abweichend zum Vorgenannten in Anlage A.

# 3 Rechte und Pflichten des Auftraggebers

**3.1** Der Auftraggeber ist gegenüber Inxmail hinsichtlich der nach dieser Vereinbarung durchgeführten Auftragsverarbeitung weisungsbefugt. Der Auftraggeber behält sich das Recht vor, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an Inxmail zu erteilen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

**3.2** Der Auftraggeber informiert Inxmail unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

**3.3** Inxmail stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der in dieser Vereinbarung (einschließlich der festgelegten technischen und organisatorischen Maßnahmen) niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen -, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden.

Kontrollmaßnahmen, Stichprobenkontrollen und insbesondere Vor-Ort-Kontrollen sind Inxmail vom Auftraggeber rechtzeitig anzukündigen und so zu gestalten, dass sie den Betriebsablauf möglichst nicht beeinträchtigen und sichergestellt ist, dass keine schutzbedürftigen Informationen von Inxmail an nicht besonders zur Verschwiegenheit verpflichtete Personen gelangen.

Fremdaufwände und über das übliche Maß hinausgehende Aufwände kann Inxmail dem Auftraggeber zu den Selbstkosten (Fremdaufwände) bzw. zu den jeweils geltenden Stundensätzen (eigene Aufwände) in Rechnung stellen.

# 4 Rechte und Pflichten von Inxmail

**4.1** Inxmail verarbeitet personenbezogene Daten nicht eigenmächtig, ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Inxmail verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Weisungsempfänger der Inxmail GmbH sind der zugeordnete Account-Manager, sowie Mitarbeiter der Kundenbetreuung, des Kundensupport oder im Rahmen von weiteren Beauftragungen jeweils benannte Mitarbeiter.

Eine Ausnahme vom Grundsatz der Weisungsgebundenheit besteht, wenn Inxmail auf Grund zwingender rechtlicher Vorschriften zur Verarbeitung der Daten (z.B. Weitergabe an Behörden etc.) verpflichtet ist. In diesem Fall teilt Inxmail dem Auftraggeber diese rechtlichen Anforderungen vor der entsprechenden Verarbeitung der Daten mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

**4.2** Soweit die Mitwirkung von Inxmail für die Beantwortung von Anträgen auf Wahrnehmung von Rechten eines Betroffenen (insbesondere auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung) erforderlich ist, wird Inxmail den Auftraggeber hierbei mit geeigneten technischen und organisatorischen Maßnahmen unterstützen.

Reichen im Einzelfall die bestehenden technischen und organisatorischen Maßnahmen nicht aus und werden erhebliche Individualaufwände erforderlich, so stellt Inxmail diese Aufwände dem Auftraggeber zu den jeweils geltenden Stundensätzen in Rechnung.

**4.3** Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat Inxmail nach Wahl des Auftraggebers sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und/oder Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers innerhalb von 30 Werktagen nach Ausübung des Wahlrechts durch den Auftraggeber datenschutzgerecht zu löschen oder dem Auftraggeber zurückzugeben.

**4.4** Inxmail ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutz-rechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen. Der Auftraggeber und Inxmail arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer gesetzlichen Pflichten zusammen.

**4.5** Inxmail unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

**4.6** Inxmail setzt bei der Durchführung der Arbeiten nur Personen ein, die auf das Datengeheimnis (Verbot der unbefugten Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten) sowie zur Vertraulichkeit verpflichtet oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

**4.7** Inxmail hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Inxmail ist berechtigt (aber nicht verpflichtet), die Durchführung

der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber schriftlich oder per Telefax bestätigt oder geändert wird.

**4.8** Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

**4.9** Die Verarbeitung von Daten des Auftraggebers in Privatwohnungen (z. B. Homeoffice der Beschäftigten des Auftragsverarbeiters) ist gestattet. Die Maßnahmen nach Art. 32 DS-GVO (siehe Anhang) sind auch in diesem Fall durch Inxmail sicherzustellen.

**4.10** Inxmail erwirbt an den Daten des Auftraggebers keine Rechte und ist auf Verlangen des Auftraggebers jederzeit auf erstes Anfordern zur Herausgabe der Daten des Auftraggebers in einer für den Auftraggeber lesbaren und weiter verarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf die Daten des Auftraggebers und die dazugehörigen Datenträger sind ausgeschlossen.

## 5 Subunternehmer

**5.1** Inxmail hat vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber den von ihm mit direktem Bezug zur Verarbeitung der personenbezogenen Daten eingesetzten Subunternehmer gelten. Zum Zeitpunkt der Beauftragung sind dies die nachfolgend aufgeführten Subunternehmer:

Bringe Informationstechnik GmbH, Zur Seeplatte 12, 76228 Karlsruhe

Sofern durch den Auftraggeber die optionale webbasierte Software Inxmail New Xperience eingesetzt wird, kommen zusätzlich nachfolgende Subunternehmer zum Einsatz:

Microsoft Ireland Operations Limited; One Microsoft Place; South County Business Park; Leopardstown; Dublin 18, D18 P521 – die webbasierte Software Inxmail New Xperience wird in einem Rechenzentrum von Microsoft (Azure) innerhalb der EU gehostet. Microsoft wendet EU Standard Vertragsklauseln an.

Interlake Media GmbH, Marlene-Dietrich-Allee 15, 14482 Potsdam, Deutschland - Der Third Level Support, der Microsoft (Azure) Komponenten wird INXMAIL durch die Interlake Media GmbH bereitgestellt.

**5.2** Inxmail darf weitere Subunternehmer im Rahmen der Auftragsverarbeitung beauftragen. Hierüber ist der Auftraggeber schriftlich zu informieren. Der Auftraggeber hat hierbei ein vierwöchiges Einspruchsrecht. Können sich der Auftraggeber und Inxmail nach Ausübung des Einspruchsrechts nicht auf eine einvernehmliche Lösung einigen, so kann jede Seite den Hauptvertrag innerhalb von 4 Wochen nach Scheitern der Verhandlungen kündigen (Sonderkündigungsrecht).

**5.3** Vor Beauftragung eines weiteren Subunternehmers schließt Inxmail durch Abschluss eines dieser Vereinbarung entsprechenden Vertrages mit dem betreffenden Subunternehmer sicher, dass die Inxmail nach dieser Vereinbarung obliegenden Datenschutzpflichten auch dem Subunternehmer auferlegt werden. Dabei stellt Inxmail insbesondere sicher, dass die gegenüber dem Subunternehmer festgelegten technisch-organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung entsprechend den gesetzlichen Vorgaben erfolgt.

## 6 Technisch-organisatorische Maßnahmen (TOMs)

**6.1** Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, des Umfangs und der Umstände der Datenverarbeitung treffen Auftraggeber und Inxmail geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die beigefügten beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

**6.2** Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es Inxmail gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber (z. B. über die Inxmail Community oder die Onlinehilfe) bekannt zu geben.

## 7 Datenschutzbeauftragte(r) von Inxmail

**7.1** Inxmail hat einen fachkundigen Datenschutzbeauftragten bestellt. Der jeweils aktuelle Datenschutzbeauftragte und die Kontaktmöglichkeiten zu diesem können auf der Webseite von Inxmail (https://www.inxmail.de/datenschutz) eingesehen werden.

## 8 Sonstiges

**8.1** Für Nebenabreden und Änderungen dieser Vereinbarung ist die Schriftform erforderlich.

**8.2** Es gilt deutsches Recht (einschließlich der EU-DSGVO), Gerichtsstand ist Freiburg im Breisgau.

**8.3** Die Einrede des Zurückbehaltungsrechts wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

**8.4** Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien werden die jeweils unwirksame Bestimmung durch eine wirksame ersetzen, die dem angestrebten Zweck möglichst nahekommt. Entsprechendes gilt, wenn eine Vertragsbestimmung undurchführbar sein oder der Vertrag eine Lücke aufweisen sollte.

**8.5** Die Parteien stellen klar, dass im Übrigen die Bestimmungen des Hauptvertrags entsprechend gelten. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag haben in Bezug auf den Datenschutz die Regelungen dieser Vereinbarung, ansonsten die Regelungen des Hauptvertrages Vorrang.

**8.6** Durch diese Vereinbarung werden alle bereits bestehenden Vereinbarungen zur Absicherung datenschutzrechtlicher Verpflichtung des Auftraggebers oder von Inxmail, insbesondere bereits in der Vergangenheit abgeschlossene Auftragsverarbeitungsvereinbarung, ersetzt.

**8.7** Es gelten die gesetzlichen Haftungsregelungen gem. Art. 82 DSGVO. Etwaige Haftungsbegrenzungen zwischen den Parteien (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung.

# Anlage A

## Art der Daten

Abweichend zu Ziffer 2.3 sind folgende Datenarten Gegenstand dieses Auftrags (bitte Zutreffendes ankreuzen):

- ☐ Personenstammdaten (z. B. Name, Adresse)
- ☐ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☐ Alter
- ☐ Bewerberdaten
- ☐ Vertrags-/Mitarbeiterstammdaten (z.B. Personal- und Identifikationsnummer)
- ☐ Lohn- und Gehaltsdaten
- ☐ Steuer-/Buchhaltungsdaten
- ☐ Arbeitszeitdaten
- ☐ Mitarbeiterbewertungen
- ☐ Mitarbeiterqualifikation und -eigenschaften
- ☐ Telekommunikationsabrechnungsdaten
- ☐ Telekommunikationsverbindungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Kundenhistorie
- ☐ Kundenverhaltensdaten
- ☐ Nutzerkennungen
- ☐ Passwörter
- ☐ Zugangsdaten
- ☐ Bankverbindungsdaten
- ☐ Kreditkartendaten
- ☐ Audiodaten
- ☐ Bilddaten
- ☐ Videodaten
- ☐ Auskunftsangaben (Auskunfteien; öffentliche Verzeichnisse etc.)
- ☐ Sonstige, und zwar (gegebenenfalls bitte nähere Angaben):

.....

## Kategorien betroffener Personen

Abweichend zu Ziffer 2.3 sind folgende Kreise von Betroffenen Gegenstand des Auftrags:

- ☐ Beschäftigte
- ☐ Auszubildende und Praktikanten
- ☐ Bewerber
- ☐ Ehemalige Arbeitnehmer
- ☐ Freie Mitarbeiter
- ☐ Gesellschafter
- ☐ Angehörige von Beschäftigten
- ☐ Kunden
- ☐ Interessenten
- ☐ Lieferanten und Dienstleister
- ☐ Mieter
- ☐ Geschäftspartner
- ☐ Berater
- ☐ Besucher
- ☐ Pressevertreter
- ☐ Abonnenten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Sonstige, und zwar (gegebenenfalls bitte nähere Angaben):

  .....

# Datenschutz-Konzept

## Technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Autor: Deutsche Datenschutzkanzlei / Inxmail GmbH



Stand Februar 2024

# Inhaltsverzeichnis

# 1 Dokumenteninformation

Das EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar. In diesem Dokument mit aufgenommen sind, die jeweils für Ihren Anwendungsfall erforderlichen technischen-organisatorischen Maßnahmen der Unterauftragnehmer. Diese sind ebenfalls nach Art. 28 DSGVO sorgfältig ausgewählt und werden laufend überprüft.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Für eine automatisierte Verarbeitung nennt die DSGVO verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit und Belastbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
5. Pseudonymisierung und Verschlüsselung
6. Kooperation mit der DDSK GmbH

# 2 Versionshistorie

| Version | Status | Datum | Verantwortlich | Änderung |
|---|---|---|---|---|
| 0.1 | Entwurf | 23.01.18 | Datenschutzbeauftragter | |
| 0.2 | Entwurf | 31.01.18 | IT-Administration | Prüfung/Anpassung |
| 0.3 | Entwurf | 08.02.18 | Datenschutzbeauftragter | Gegenprüfung/Ergänzung |
| 1.0 | Initialversion | 09.02.18 | Datenschutzkoordination | Gegenprüfung/Ergänzung |
| 1.1 | Version | 04.12.2019 | Datenschutzkoordination | Prüfung/Anpassung |
| 1.2 | Version | 06.07.2020 | Datenschutzkoordination | Prüfung/Anpassung |
| 1.3 | Version | 15.01.2022 | Datenschutzkoordination | Prüfung/Anpassung |
| 1.4 | Version | 23.09.2022 | Datenschutzkoordination | Prüfung/Anpassung |
| 1.5 | Version | 15.08.2023 | Datenschutzkoordination | Prüfung/Anpassung |

| | | | | |
|---|---|---|---|---|
| 1.6 | Version | 20.02.2024 | Datenschutzkoordination | Prüfung/Anpassung |

# 3 Organisatorisches

Die Inxmail GmbH arbeitet mit der Deutschen Datenschutzkanzlei zusammen und wird in allen datenschutzrechtlichen Fragen von Herrn Stefan Fischerkeller und Herrn Marius Bernhardt beraten. Herr Fischerkeller ist bestellter, externer Datenschutzbeauftragter nach Art. 37 DSGVO der Inxmail GmbH. Die Deutsche Datenschutzkanzlei führt regelmäßig Überwachungsaudits, sowie fachspezifische Schulungen durch und stellt Richtlinien, Handlungshilfen und gelenkte Dokumente zur Verfügung.

Die Inxmail GmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus, sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Zudem sind Verfahren im Bereich Benachrichtigung, Auskunftsersuchen sowie Anliegen zur Berichtigung, Löschung und Sperrung implementiert. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis sowie die Vertraulichkeit verpflichtet. Beschäftigte, die an der Erbringung von Telekommunikationsdienstleistungen mitwirken, sind zusätzlich auf das Fernmeldegeheimnis nach § 3 des Telekommunikation-Telemedien-Datenschutz-Gesetz - TTDSG verpflichtet.

# 4 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der Inxmail GmbH betrieben werden. Die Server und Datenbanken sowie die Datensicherung (Backup) aller ADV-relevanten Daten werden in einem professionell betriebenen Rechenzentrum gehostet und gewartet. Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden. Die Unterbeauftragten werden sorgfältig ausgewählt und hinsichtlich ihres Sicherheitsbewusstseins und ihrer Fachkompetenz überprüft.

## 4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

### 4.1.1 Zutrittskontrolle Unternehmensräumlichkeiten

› Es wird dem Schutzbedarf der Daten angemessenes Schließsystem verwendet (Schlüssel; Chipkarten-/Transponder-Schließsystem).

› Kontrollierte und dokumentierte Vergabe elektronischer Schlüssel (sog. Transponder) zur Kontrolle des Zutritts zu den Büroräumen, Protokollierung (Uhrzeit, Datum, Person) Alarm scharf/unscharf geschaltet, bzw. Auslöser.

- Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
- Eine Dokumentation der Schlüsselvergabe wird geführt und laufend aktualisiert.
- Das Gebäude ist verschlossen und kann nur manuell durch die Mitarbeiter geöffnet werden.
- Sicherung der Büro-/Geschäftsräume während der Arbeitszeit über den zentralen Empfang, der während der Bürozeiten (Mo-Do 8:30-17:30 Uhr; Fr. 8:30-17:00) durchgehend besetzt ist. An diesem müssen sich die Besucher anmelden, und werden dann von einem Mitarbeiter abgeholt.
- Besucher halten sich ausschließlich in Begleitung eines Mitarbeiters im Gebäude auf.
- Besucher werden im Besucherbuch registriert und erhalten einen Besucherausweis.
- 24/7-Überwachung des Firmengeländes und Büroräumlichkeiten durch einen Sicherheitsdienst und interne Alarmbereitschaft.
- Weitere Schutzmaßnahmen sind implementiert (Lichtschranken-/Bewegungsmelder; Alarmanlage; Kamera an der Tür; Gegensprechanlage zur Öffnung der Eingangstür).
- Alarmauslösung bei unberechtigten Zutrittsversuchen über sämtliche mögliche Eingänge und Fenster.
- Ein abschließbares Archiv sowie abschließbare Schränke sind vorhanden. Restriktive Zugriffsberechtigungen kommen zum Einsatz. Die Schlüssel stehen nur den Berechtigten zur Verfügung.
- Das Gebäude ist mit Sicherheitsverglasung ausgestattet.
- Notfall-/Incidentmanagement nach BSI 100-4 und ISO 27001 ist vorhanden.
- Notfall/-Incidentmanagement bei Zutrittsverletzungen laut Eskalationsplan, nach BCM ISO 27001.

### 4.1.2 Zutrittskontrolle externe Serverräume

- Die Zutrittskontrolle zu den Serverräumen wird durch die räumliche Struktur und die eingesetzten Kontrollsysteme gewährleistet (Unterteilung Rechenzentrum in verschiedene Zugangsbereiche, die durch Schleusen mit dem Eingangsbereich verbunden sind). Für das Betreten und Verlassen der Sicherheitsbereiche und des Gebäudes ist ein festes Vorgehen festgelegt. Verstöße lösen automatisch Alarm aus, der Sicherheitsdienst, Polizei und Feuerwehr alarmiert.
- Die Zutrittsberechtigung zu den Rechenzentren erfolgt restriktiv (ausschließlich IT-Administration; Techniker). Zusätzliche Sicherung des Serverraumes und der Netzwerktechnik durch einen Transponder, auf den nur die Administratoren Zugriff haben. Andere Betriebsangehörige bzw. Betriebsfremde erhalten nur unter Aufsicht Zugang.

- Die Rechenzentren verfügen über ein automatisiertes, elektronisches Zutrittssystem mit Protokollierung der Zutritte, einem dreifachen Zugangsverfahren (Transponder, personalisierte Code-Schlüssel, PIN-Felder) sowie Kameraüberwachung.
- Die Racks in den Rechenzentren sind abgeschlossen.
- Netzwerkkomponenten werden in nicht öffentlich zugänglichen Bereichen sowie abschließbaren Schränken betrieben.
- Das Gelände wird durch einen Wachdienst kontinuierlich inspiziert. Von Wachdienst angetroffene Personen müssen sich ausweisen und Ihre Anwesenheitsberechtigung vorlegen.
- Besucher halten sich ausschließlich in Begleitung eines Mitarbeiters im Rechenzentrum auf.
- Zutritte und Arbeiten werden stets dokumentiert und protokolliert.
- Der Hosting-Dienstleister ist ISO 27001 zertifiziert.

### 4.1.3 Zugangskontrolle

- Verbindliches Verfahren zu Vergabe und Entzug von Berechtigungen:
- Regelung des Zugangs zu den DV-Systemen über ein Benutzer-/Berechtigungskonzept.
- Vergabe personalisierter Benutzeraccounts und Hardware mit entsprechenden Kennwortrichtlinien (eindeutige Zuordnung Benutzerkonten zu Benutzern). Zuordnung Mitarbeiter in eine oder mehrere Benutzergruppen, wobei die jeweiligen Benutzergruppen unterschiedliche Zugriffsrechte haben (Rechtebeschränkung Standardnutzer).
- Protokollierung fehlerhafter Passworteingaben. Auswertung Protokolle bei Auffälligkeiten.
- Netzdienste werden nur im Rahmen der für die Aufgabe erforderlichen Nutzungsszenarien vergeben. Berechtigungen sind zentral über ein Identity and Access Management Service geregelt.
- Die Datenübertragung von und zu den DV-Systemen wird bei kritischen Aktivitäten (z.B. bei Systempflege, Softwareupdates, Backups, Fernwartung) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert:
  - Überprüfung bekannter öffentlicher Schlüssel bei Kontaktaufnahme.
  - Verschlüsselte Datenübertragung (TLS/SSH).
  - Zugriff auf System von außen über VPN-Verbindung.
  - Protokollierung der Systemnutzung.
  - Zugang Fernwartungspersonal nur über personalisierte SSH-Keys.
- Fernwartungsmaßnahmen werden überwacht und können jederzeit abgebrochen werden.

- Eine Kennwortrichtlinie mit Vorgaben für den Passwort-Standard ist implementiert:
- Länge und Komplexität des Passwortes orientieren sich nach den aktuellen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik. Zeitliche Sperrung nach 10-maliger Falscheingabe. Bei eventuellem Bekanntwerden eines Passwortes muss dieses umgehend geändert werden und es erfolgt eine Meldung an die verantwortliche IT-Fachabteilung sowie die Sperrung aller betroffenen Zugänge und Endgeräte. Die definierten Passwortregelungen, werden in den zentralen Systemen technisch erzwungen.
- Einsatz von Firewalls zur Verhinderung von Angriffen. Systeme werden in unterschiedlichen Netzwerksegmenten betrieben, die mittels Firewall-Regelungen voneinander getrennt sind. Das Unternehmensnetzwerk ist durch eine umfassende Firewall-Architektur gegen Angriffe gesichert.
- Spamfilter und Virenschutzprogramme sind vorhanden und werden immer auf dem aktuellsten Stand gehalten.
- Content Filter und Einsatz von Reverse Proxy zum Schutz der Applikationen und Netzwerke
- Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe) und Abschaltung von überflüssigen Diensten.
- Es ist ein umfassendes Netzwerkmonitoring (mit 24/7-Kontrolle) mit entsprechenden Alarmierungen (Bereitschaftsdienst außerhalb Geschäftszeiten) etabliert.
- Beschränkung der Server in den Rechenzentren auf die benötigten Dienste.
- Protokollierung von Systemnutzungen und verfügbare Logs
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten/Remote-Zugriff).
- Abschaltung von überflüssigen Diensten.
- Verschlüsselung von Datenträgern und Notebooks.
- Spamfilter für Maileingang.~~,~~ Spamfilter und Virenschutzprogramme sind vorhanden und werden immer auf dem aktuellsten Stand gehalten.
- Sämtliche Arbeitsstationen werden bei Verlassen des Arbeitsplatzes vom Benutzer oder nach Inaktivität gesperrt (passwortgeschützte, automatische Bildschirmsperren).
- Reduktion der zugriffsberechtigten Personen auf ein Minimum.
- Jährliche Penetrationstests werden vorgenommen.

### 4.1.4 Zugriffskontrolle

› Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:

  – Vergabe von personalisierten Benutzeraccounts und personalisierter Hardware mit entsprechenden Kennwortrichtlinien (eindeutige Zuordnung von Benutzerkonten zu Benutzern).

  – Zuordnung der Mitarbeiter in eine oder mehrere Benutzergruppen, wobei die jeweiligen Benutzergruppen unterschiedliche Zugriffsrechte haben (Rechtebeschränkung Standardnutzer).

  – Differenzierte Zugriffsberechtigung auf Anwendungsprogramme.

  – Differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen).

› Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern wird verhindert durch:

  – Datenträgerverwaltung-/Management.

  – Benennung Verantwortliche für die Herausgabe/Prüfung von Hardware/Datenträgern.

  – Softwareseitigen Ausschluss (Berechtigungskonzept).

  – Konzept zur Laufwerksnutzung/-zuordnung

  – Gesicherte Schnittstellen.

› Ein verbindliches Verfahren zur Vergabe von Berechtigungen ist implementiert (verbindliches Administrationskonzept). Restriktive Zugriffsberechtigung/projektbezogene Zugänge inkl. Logging/Protokollierung. Die Beantragung und Vergabe von Berechtigungen erfolgt unter Einbeziehung des Vorgesetzten und mit Dokumentation der Berechtigungsvergabe im Directory Service.

› Personifizierte Admin-Account mit erhöhten Kennwortvorgaben (Zwölf Zeichen: Groß-/Kleinbuchstaben; Zahlen).

› Einsatz IT-Sicherheitsrichtlinie/Policies (u.a. Nutzung von Wechselmedien; Umgang mit personenbezogenen Daten/Kundendaten, Passworteinsatz/-vorgaben, Verschlüsselung, Ablage/Speicherung von Daten etc.).

› Verbot Einsatz private Datenträger.

### 4.1.5 Trennungsgebot

› Zwischen Test- und Produktionsumgebung gibt es eine Trennung mit Firewalls und dedizierten Datenbankservern und Applikationsserverinstanzen.

› Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden. Die unterschiedliche und getrennte Verarbeitung wird gewährleistet durch:

- Softwareseitigen Ausschluss (Mandantentrennung im ASP Service).
- Datenbankprinzip, Trennung über Zugriffsregelung.
- Trennung von Test- und Produktivdaten (Produktivdaten ausschließlich in ISO 27001-Hosting-Dienstleister).
- Funktionstrennung.
- Trennung von Entwicklungs- und Produktionsprogrammen.
- Logische Trennung.
- Speicherung unterschiedlicher Datenkategorien in getrennten Datenbanken und Verarbeitung je nach Verwendungszweck mit geeigneter Software.

## 4.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 4.2.1 Weitergabekontrolle

› Ein physischer Versand von Datenträgern ist nicht vorgesehen.

› Verbot des Einsatzes privater Datenträger.

› Nicht mehr benötigte Datenträger werden durch Dienstleister zerstört (magnetisch).

› Laptops sind verschlüsselt.

› Alle zum Transport oder für die Übertragung vorgesehenen sensitiven Daten werden verschlüsselt.

› Der Schutz personenbezogener Daten beim physischen Transport bzw. bei der elektronischen Übermittlung wird durch folgende Maßnahmen sichergestellt:

- VPN
- Anonymisierungs-/Pseudonymisierungsverfahren
- Verschlüsselung Datenträger
- Ausschließliche Nutzung von durch die IT freigegeben Systeme
- Verschlüsselte Verbindungen per Default (SFTP, HTTPS, TLS ...)

› Folgende Sicherheitsmaßnahmen existieren:

- Hardware- und Software-Firewall
- Programme, die das Eindringen von Viren verhindern bzw. das Eindringen erkennen
- Erkennung und Markierung von SPAM

- Nur freigegebene Dienste dürfen genutzt werden (technisch erzwungen und per Policy umgesetzt).
- Kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN-Norm 66399 mit Sicherheitsstufe 4 oder höher (direkt vor Ort von zertifiziertem Dienstleister oder durch Abholung).
- Für mobile Arbeitsplätze und Heimarbeitsplätze existieren VPN-Zugänge zum Unternehmensnetzwerk.
- Vorgegebene Datenträgerverwaltung mit Bestandsüberwachung/-kontrolle (Vollständigkeits- und Richtigkeitsprüfung). Gesicherter Eingang für An- und Ablieferung.
- Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege.
- Eine Richtlinie zum Umgang mit technischen Zertifikaten ist implementiert.
- Mandanten sind voneinander getrennt.
- Informationen sind nach Vertraulichkeitsstufen klassifiziert gem. ISMS Richtlinie nach ISO 27001.

### 4.2.2 Eingabekontrolle

- Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:
  - Benutzerprofile.
  - Benutzeridentifikation.
  - Berechtigungskonzepte.
  - In zentralen Systemen werden Logfiles geführt, die Eingaben und Veränderungen an Daten nachvollziehbar machen.
  - Protokollierung eingegebener Daten (Verarbeitungsprotokoll). Insbesondere Protokollierung gescheiterter Anmeldeversuche.
  - Protokollierung der Eingabe, Änderung und Löschung von Daten.
  - Zentrale Log-Server.
  - Protokollierung administrative Tätigkeiten im Directory Service.
- Die Inxmail GmbH erhebt, verändert oder löscht personenbezogene Daten primär im Rahmen der eigenen Kundenverwaltungssysteme (Bestands-; Nutzungsdaten; Endkundendaten) bzw. nur im Auftrag/ nach Weisung des Kunden/Auftraggebers.
- Im Rahmen der (Fern-)Wartung erfolgt eine Zugriffsprotokollierung der Tätigkeiten von Inxmail via HTTPS, VPN und/oder System Logs

› In zentralen Systemen werden Logfiles geführt, die Eingaben und Veränderungen an Daten nachvollziehbar machen. Die Konfiguration des Logs-auswertung und -bearbeitung Tools ist versioniert und revisionssicher hinterlegt

### 4.2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

› Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch:

- Einsatz von RAID-Festplattensystemen.
- Einsatz von USV inkl. Überspannungsschutz und Notstromaggregat (zwei unabhängige Generatoren, die Energieversorgung bei mehrtägiger Stromunterbrechung gewährleisten können).
- Blitzschutzeinrichtungen.
- Feuer- und Rauchmeldeanlagen mit Löschanlage (ARGON-Gas; Sauerstoffverdrängung).
- Brandfrüherkennungssystem (Brandgas-Schnüffel-System: Früherkennung Überhitzungs-schäden vor Brand; Auslösung Voralarm; Verhinderung Ausbreitung) und normale Brandmeldeanlage.
- Betrieb einer Alarmanlage inkl. Weiterleitung an Leitstelle, Werkschutz, Feuerwehr, Wachdienst etc. (Feuerwehr 500m Entfernung zu Rechenzentrum). Mit Auslösung Alarm wird Bereich automatisch spannungsfrei geschaltet.
- Einsatz unterschiedlicher Sensoren zur Identifikation von physischen Beeinträchtigungen (Wasser, Temperatur, Luftfeuchtigkeit etc.: doppeltes Verfahren: Sensoren RZ und separates Kontrollsystem). Einsatz Klimaanlage inkl. Dokumentation Klimatechnik.
- Einsatz eines Wachdienstes.
- Mehrfache Datenbank- und Systembackups.
- Alle wichtigen DV-Systeme werden vom Back-Up-System abgedeckt.
- Die Netzwerkarchitektur ist so ausgelegt, dass eine Redundanz stets gewährleistet ist.
- Konzept zur Rekonstruktion der Datenbestände (IT-/Desaster-Recovery).
- Verteilung Netzwerkkomponenten zum Zweck der Risiko-/Ausfallminimierung auf mehrere geschützten Bereiche. Aufbewahrung der Sicherungen geographisch getrennt voneinander.
- Personaldatenarchiv, Backups in anderen Aufbewahrungsorten-Brandabschnitte.
- CCollect, Tape im Schließfach, dezidierte Backupserver, Infrastruktur Systeme sind redundant.
- Bestellung eines Informationssicherheitsbeauftragten
- Virenschutzprogramme/Anti-Malwareprogramme sind vorhanden und aktuell.

- Einsatz eines unternehmensweit gültigen ISMS.
- Ein Business Continuity Management System nach ISO 27001 ist vorhanden.
- Maßnahmen gegen DOS-Angriffe durch den eingesetzten Infrastrukturdienstleister.

## 4.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

### 4.3.1 Datenschutz-Management und ISO 27001

Die Inxmail GmbH wird von der Deutschen Datenschutzkanzlei (externer Datenschutzbeauftragter: Stefan Fischerkeller) im Bereich Datenschutz betreut. Die Deutsche Datenschutzkanzlei führt für die Inxmail GmbH ein Datenschutzmanagementsystem, in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen. Das DSMS wird von der Deutschen Datenschutzkanzlei laufend gepflegt und aktualisiert.

Die Inxmail GmbH ist als Unternehmen nach ISO 27001 zertifiziert. Es erfolgt eine jährliche Rezertifizierung und Überprüfung der ISO 27001 Maßnahmen und Standards.

### 4.3.2 Incident-Response-Management

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (Incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen, eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

Die Rollen und Aufgaben im Rahmen des Incident-Response-Management sind nach BSI 100-4 und nach ISO 27001innerhalb des ISMS definiert, dessen oberstes Ziel der Schutz der Informationen sowie die schnellstmögliche Wiederherstellung der Infrastruktur/ Servicedienstleistung im Schadensfall ist.

## 4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden. Die Softwarelösungen der Kunden können von diesen selbst angepasst und verwaltet werden. Eine Löschung/Berichtigung der Daten im System seitens des Kunden ist immer möglich. Applikation Lifecycle Management ist Teil des unternehmensweiten Produktmanagement-Prozess. Es stellt einen Leitfaden zur Entwicklung von Anwendungen konform zu dem bestehenden ISMS dar und dient somit der Erfüllung der ISO 27001.

### 4.5. Auftragskontrolle

Die Mitarbeiter sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert/unterzeichnet.

Sollte die Inxmail GmbH bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO i.V.m. Art 32 Abs. 1 DSGVO. Folgende Voraussetzungen für ein Unterauftragsverhältnis gelten:

- Es bestehen detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe des Art. 28 Abs. 3 DSGVO. Die entsprechenden Angaben sind vertraglich fixiert.
- Deutsche Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt, sofern eine Bestellung gesetzlich vorgeschrieben ist und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Eine regelmäßige Prüfung der beauftragten Unternehmen erfolgt durch den eigenen die interne IT-Administration, den Datenschutzbeauftragten oder den IT-Sicherheitsbeauftragten.
- Mündliche Aufträge müssen schriftlich bestätigt und dokumentiert werden.
- Eine Vergabe von Einzelaufträgen erfolgt nur über namentlich benannte Ansprechpartner.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitungsvereinbarung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

## 5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Im Rahmen der Verarbeitung von personenbezogenen Daten kommen verschiedene Verschlüsselungsmechanismen (bspw. TLS/SSH-Verschlüsselung bei Übertragung; externer Zugriff per VPN) zum Einsatz. Zudem werden die Kundendaten auf den Datenverarbeitungssystemen pseudonymisiert (Kundennummer), um einen noch höheren Schutz der Daten zu gewährleisten.

# 6 Kooperation mit der Deutschen Datenschutzkanzlei; DDSK GmbH

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach BDSG bzw. der ab dem 25.05.2018 geltenden EU-Datenschutzgrundverordnung, arbeitet die Inxmail GmbH mit der Deutschen Datenschutzkanzlei zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen, berät die Deutsche Datenschutzkanzlei die Inxmail GmbH in allen Fragen rund um den Datenschutz und stellt mit Herrn Stefan Fischerkeller den externen Datenschutzbeauftragten nach Art. 37 DSGVO des Unternehmens.

Ansprechpartner der Deutschen Datenschutzkanzlei sind:

**Stefan Fischerkeller**
Diplomverwaltungswirt (FH), geprüfter fachkundiger Datenschutzbeauftragter (DESAG)

**Marius Bernhardt**
Consultant, Wirtschaftsjurist (LL.B), geprüfter fachkundiger Datenschutzbeauftragter (DEKRA)

DDSK GmbH
Dr.-Klein-Straße 29, 88069 Tettnang
Tel. 07542 / 949 21 00
E-Mail: datenschutz@inxmail.de
www.ddsk.de

DEUTSCHE DATENSCHUTZ KANZLEI

Kontakt Inxmail GmbH
datenschutz@inxmail.de; https://www.inxmail.de/datenschutz; Tel. 0761 / 296979-0