

Datenschutzerklärung

1. Einleitung und Geltungsbereich	4
a. Zweck der Datenschutzerklärung	
b. Geltungsbereich	
c. Rechtsgrundlagen	
2. Verantwortliche	5
a. Angaben zum Verantwortlichen	
b. Kontakt Datenschutzbeauftragter oder Datenschutzkoordination	
3. Begriffe	6
a. Personenbezogene Daten	
b. Verarbeitung	
c. Verantwortlicher	
d. Auftragsverarbeiter	
e. Empfänger	
f. Drittland oder internationale Organisation	
g. Einwilligung	
h. Kundenkonto, Benutzerkonto, aktiver Nutzer	
i. Dienst, Plattform, Cloud Services	
4. Verarbeitungszwecke und Datenkategorien	7
a. Websitebesuch und Server-Logfiles	
b. Registrierung und Kundenkonto	
c. Vertragsdurchführung und Nutzung der Plattform	
d. Kommunikation, Support und Ticketsystem	
e. Zahlungsabwicklung	
f. Newsletter und Marketingkommunikation	
g. Kundenakquise im B2B Bereich	
h. Bewerbungen	
i. Sicherheitsmaßnahmen und Missbrauchserkennung	
j. Analyse, Statistik und Reichweitenmessung	
k. Cookies und vergleichbare Technologien	
l. Verarbeitung von Unternehmensdaten, Mitarbeiterdaten und geschützten Inhalten innerhalb des Kundenkontos	
5. Rechtsgrundlagen der Verarbeitung	9
a. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung)	
b. Art. 6 Abs. 1 lit. b DSGVO (Vertrag und vorvertragliche Maßnahmen)	
c. Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)	

- d. Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Verpflichtung)
- e. TTDSG (Deutschland) bei Cookies und Tracking

6. Datenverarbeitung im Rahmen der Plattformnutzung 10

- a. Verarbeitete Daten der Nutzerkonten
- b. Teamverwaltung, Rollen und Berechtigungen
- c. Verarbeitete Dokumente und Dateien im Dokumentenspeicher
- d. Aktivitätsdaten, Logs und Audit Trails
- e. Backup, Restore und Archivierung
- f. Datenlöschung und Speicherfristen
- g. Mandantentrennung und Verschlüsselung

7. Zahlungsdaten 12

- a. Zahlungsarten und gespeicherte Daten
- b. Übermittlung an Zahlungsdienstleister
- c. Identitäts und Betrugsprüfung
- d. Löschfristen für Zahlungsdaten

8. Cookies und Tracking Technologien 13

- a. Technisch notwendige Cookies
- b. Funktionale Cookies
- c. Statistik und Analyse
- d. Marketing und Personalisierungs Cookies
- e. Cookie Einstellungen und Widerruf
- f. Kontaktformular / Rückruf-Service

9. Analyse- und Marketing-Tools 14

- a. Google Analytics
- b. Google Tag Manager
- c. Newsletter-Tracking
- d. Opt-Out-Mechanismen
- e. HR-Expertise (Newsletter)
- f. Kundenakquise / B2B-Direktwerbung

10. Einbindung von Diensten Dritter 16

- a. Google Maps
- b. YouTube
- c. reCAPTCHA
- d. CDN-Dienste (Cloudflare oder andere)
- e. Weitere Drittanbieter

11. Hosting 17

- a. Hostinganbieter (Strato)
- b. Logfiles
- c. Unterauftragnehmer
- d. Geografische Datenlokation

e. AVV mit Hostingpartnern	
12. Auftragsverarbeiter und Unterauftragsverarbeiter	18
a. Kategorien von Auftragsverarbeitern	
b. Subunternehmerliste	
c. Prüf- und Kontrollrechte	
d. Datenübermittlung in Drittstaaten	
e. Garantien (Standardvertragsklauseln etc.)	
13. Datenübermittlung an Dritte	19
a. Zweckgebundene Übermittlung	
b. Übermittlung an Zahlungsanbieter	
c. Übermittlung an Behörden	
d. Kein Verkauf oder Vermietung von Daten	
e. Forderungsdurchsetzung und Inkasso	
f. Automatisierter Datenexport an externe Buchhaltungssysteme und Steuerberater	
g. Nutzung externer Speicheranbieter durch den Kunden (Bring Your Own Storage)	
14. Internationale Datenübermittlung	20
a. EU / EWR	
b. Drittstaatentransfer	
c. Rechtsgrundlagen für Übermittlung in die USA	
d. Sicherungsmechanismen (SCC, Art. 46 DSGVO)	
15. Datensicherheit / Technische und organisatorische Maßnahmen (TOMs)	21
a. Verschlüsselung (Transport, Ruhe)	
b. Zugriffsbeschränkung / Zugriffskontrolle	
c. Protokollierung und Monitoring	
d. Physische Sicherheit	
e. Backup-Strategie	
f. Penetrationstests / Sicherheitsüberprüfungen	
g. Incident Response und Meldeprozesse	
16. Rechte der betroffenen Personen	22
a. Auskunft	
b. Berichtigung	
c. Löschung	
d. Einschränkung	
e. Widerspruch	
f. Datenübertragbarkeit	
g. Widerruf	
h. Beschwerderecht bei der Aufsichtsbehörde	
17. Löschfristen und Speicherdauer	23
a. Gesetzliche Aufbewahrungsfristen	
b. Kundendaten	

c. Vertragsdaten	
d. Plattformdaten und E-Rechnungs-Archivierung	
e. Logfiles	
f. Backups	
18.Minderjährige	24
a. Nutzung nur durch Erwachsene	
b. Ausschluss aktiver Erfassung	
19.Änderungen der Datenschutzerklärung	25
a. Änderungsrechte	
b. Benachrichtigung der Nutzer	
20.Kontakt	25
a. Kontaktstelle für Datenschutz	
b. Beschwerden, Anliegen und Anfragen	

1. Einleitung und Geltungsbereich

a. Zweck der Datenschutzerklärung

Diese Datenschutzerklärung beschreibt, wie Hyptime personenbezogene Daten verarbeitet, wenn Nutzer unsere Website, die cloudbasierte Plattform oder weitere digitale Dienste verwenden. Sie legt offen, welche Daten wir erheben, zu welchen Zwecken wir sie nutzen, auf welcher rechtlichen Grundlage dies geschieht und welche Rechte Nutzer im Zusammenhang mit ihren Daten haben. Ziel ist es, die Verarbeitungsvorgänge transparent darzustellen und sicherzustellen, dass alle gesetzlichen Anforderungen, insbesondere der DSGVO, eingehalten werden.

b. Geltungsbereich

Diese Datenschutzerklärung gilt für alle datenverarbeitenden Vorgänge, die im Zusammenhang mit den Angeboten und Diensten von Hyptime stehen. Dazu gehören:

- Website unter sämtlichen Domains und Subdomains
- Hyptime Business Suite (Cloud Plattform)
- Mobile Anwendungen

- Hyptime API Schnittstellen
- Supportportale, Ticket Systeme und Dokumentationsplattformen
- Kommunikationskanäle wie E-Mail, Chat, Telefon, Kontaktformulare und Rückrufservices
- Marketingmaterialien, Newsletter und Veranstaltungen
- Kundenbereich und Benutzerkonten
- Integrationen von Drittanbietern, sofern sie durch Hyptime kontrolliert eingebunden sind

Soweit über unsere Plattform Daten im Auftrag unserer Kunden verarbeitet werden, erfolgt diese Verarbeitung ausschließlich gemäß den Vorgaben eines Auftragsverarbeitungsvertrags.

c. Rechtsgrundlagen

Die Verarbeitung personenbezogener Daten durch Hyptime stützt sich auf die folgenden gesetzlichen Grundlagen:

- DSGVO als zentrale europäische Datenschutzverordnung
- Bundesdatenschutzgesetz für ergänzende nationale Vorschriften
- TTDSG für den Einsatz von Cookies, Trackingtechnologien und Telemediendienste
- Handels- und steuerrechtliche Vorschriften für Aufbewahrungspflichten

Je nach Verarbeitungsvorgang erfolgt die Datenverarbeitung aufgrund von Einwilligungen, Vertragserfüllung, gesetzlicher Verpflichtung oder berechtigten Interessen.

2. Verantwortliche

a. Angaben zum Verantwortlichen

Verantwortlich für die Verarbeitung personenbezogener Daten im Sinne der Datenschutzgesetze ist:

Hyptime – Software Engineering
 Erdal Cosgun
 Hessische Straße 166
 44339 Dortmund
 Deutschland

Telefon: +49 231 8802 5269

E-Mail: info@hyptime.com

Der Verantwortliche entscheidet über Zwecke und Mittel der Verarbeitung personenbezogener Daten innerhalb der Website, Plattform und sämtlicher zugehöriger Dienste.

b. Kontakt Datenschutzbeauftragter oder Datenschutzkoordination

Für alle Fragen zum Datenschutz sowie zur Ausübung Ihrer gesetzlichen Betroffenenrechte steht Ihnen unsere interne Datenschutzkontaktstelle unter info@hyptime.com zur Verfügung.

Sofern nach Art. 37 DSGVO die Bestellung eines Datenschutzbeauftragten erforderlich wird oder freiwillig erfolgt, werden die entsprechenden Kontaktdaten an dieser Stelle aktualisiert.

3. Begriffe

Zur besseren Verständlichkeit werden die wichtigsten datenschutzrechtlichen Begriffe im Sinne der DSGVO definiert.

a. Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu zählen etwa Name, E-Mail-Adresse, Telefonnummer, IP-Adresse, Standortdaten, Nutzerkennungen oder alle Informationen, die einer Person direkt oder indirekt zugeordnet werden können.

b. Verarbeitung

Verarbeitung umfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten, unabhängig davon, ob er automatisiert erfolgt. Dazu gehören insbesondere Erheben, Erfassen, Speichern, Anpassen, Übermitteln, Abgleichen, Einschränken, Löschen und Vernichten.

c. Verantwortlicher

Der Verantwortliche ist die natürliche oder juristische Person, Behörde oder sonstige Stelle, die allein oder gemeinsam mit anderen über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

d. Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde oder sonstige Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, etwa Hosting-Anbieter, Cloud-Dienste oder Support-Dienstleister.

e. Empfänger

Ein Empfänger ist jede Person oder Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich um Dritte oder verbundene Unternehmen handelt. Behörden gelten nur dann als Empfänger, wenn sie Daten im Rahmen eines konkreten Ermittlungsverfahrens erhalten.

f. Drittland oder internationale Organisation

Ein Drittland ist jeder Staat außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums. Eine internationale Organisation ist eine zwischenstaatliche Einrichtung wie die Vereinten Nationen. Für Datenübermittlungen in diese Bereiche gelten besondere Schutzmechanismen nach Kapitel V DSGVO.

g. Einwilligung

Einwilligung ist jede freiwillige, informierte und unmissverständlich abgegebene Willensbekundung der betroffenen Person, mit der sie durch eine Erklärung oder eine eindeutig bestätigende Handlung in die Verarbeitung ihrer personenbezogenen Daten einwilligt.

h. Kundenkonto, Benutzerkonto, aktiver Nutzer

Ein Kundenkonto oder Benutzerkonto ist ein individueller Zugang zur Plattform von Hyptime, der zur Nutzung der bereitgestellten Cloud Services erforderlich ist.

Ein aktiver Nutzer ist ein Benutzerkonto, das genutzt oder technisch aktiviert ist und im Rahmen der Lizenzmodelle abrechnungsrelevant wird.

i. Dienst, Plattform, Cloud Services

Dienst, Plattform oder Cloud Services bezeichnet die von Hyptime bereitgestellten webbasierten Softwarelösungen einschließlich aller Module, Schnittstellen, Subdomains, administrativen Funktionen und unterstützenden Systeme.

4. Verarbeitungszwecke und Datenkategorien

Hyptime verarbeitet personenbezogene Daten nur, soweit dies für den Betrieb der Website, die Bereitstellung der Cloud Services und die Erfüllung vertraglicher sowie gesetzlicher Pflichten erforderlich ist. In den folgenden Abschnitten wird erläutert, welche Daten in welchem Zweck verarbeitet werden.

a. Websitebesuch und Server-Logfiles

Beim Aufruf der Website werden automatisch Daten verarbeitet, die für den technischen Betrieb und die Sicherheit erforderlich sind. Dazu gehören IP-Adresse, Datum und Uhrzeit des Zugriffs, aufgerufene Seiten, übertragene Datenmenge, Browsertyp, Betriebssystem, Referrer-URL und technische Fehler. Diese Daten dienen der Stabilität, Sicherheit, Störungsanalyse und Missbrauchserkennung. Eine Zuordnung zu einer Person erfolgt nur bei Vorfällen wie Angriffen.

b. Registrierung und Kundenkonto

Für die Erstellung und Verwaltung eines Kundenkontos werden Stammdaten wie Name, Unternehmensangaben, Adresse, E-Mail-Adresse, Telefonnummer und Login-Daten verarbeitet. Zusätzlich werden Rechte, Rollen und interne Benutzerzuordnungen gespeichert. Diese Informationen sind erforderlich, um den Zugang zur Plattform zu ermöglichen und den Vertrag zu erfüllen.

c. Vertragsdurchführung und Nutzung der Plattform

Während der Nutzung der Plattform verarbeitet Hyptime personenbezogene Daten der Nutzer, etwa Nutzungsdaten, Metadaten, Änderungsprotokolle und Inhalte, die Kunden selbst einstellen. Dazu gehören Dokumente, Einträge, Kommunikationsdaten, Uploads, Profilbilder und interne Organisationsinformationen. Die Verarbeitung erfolgt zur Bereitstellung der Funktionen, Speicherung von Inhalten, Synchronisation, Workflows, Sicherheit und Abrechnung.

d. Kommunikation, Support und Ticketsystem

Bei Kontaktanfragen, Supporttickets oder Kommunikation per E-Mail, Chat oder Telefon werden die übermittelten Daten (Kontaktdaten, Inhalte der Anfrage, technische Informationen) verarbeitet. Der Zweck ist die Bearbeitung der Anfrage, Fehleranalyse und Dokumentation.

Hinweis zum Support-Zugriff: Zur schnellen und zielgerichteten Fehlerbehebung kann es erforderlich sein, dass autorisierte Support-Mitarbeiter von Hyptime temporären Lesezugriff auf das Benutzerkonto und die Konfigurationen des Kunden nehmen. Durch das explizite Eröffnen eines Support-Tickets oder die Anforderung von technischer Hilfeleistung willigt der Kunde in diesen temporären, zweckgebundenen Zugriff gemäß Art. 6 Abs. 1 lit. b und f DSGVO ein. Dieser Zugriff wird protokolliert und strikt auf das zur Fehlerbehebung notwendige Minimum beschränkt.

e. Zahlungsabwicklung

Für kostenpflichtige Leistungen verarbeitet Hyptime Zahlungsdaten wie Rechnungsadresse, Buchungsdaten, gewählte Zahlungsmethode und Zahlungsstatus. Abhängig vom Zahlungsdienstleister können zusätzlich Daten an Zahlungsanbieter übermittelt werden. Diese Verarbeitung ist notwendig für Abrechnung, Rechnungsstellung, Buchhaltung und Vertragserfüllung.

f. Newsletter und Marketingkommunikation

Für den Versand von Newslettern und Marketinginformationen werden Kontaktdaten wie Name und E-Mail-Adresse verarbeitet. Diese Verarbeitung erfolgt nur nach Einwilligung. Darüber hinaus wird gemessen, ob E-Mails zugestellt, geöffnet oder angeklickt wurden, um Inhalte zu optimieren. Eine Abmeldung ist jederzeit möglich.

g. Kundenakquise im B2B Bereich

Im Rahmen der Geschäftsanbahnung verarbeitet Hyptime öffentlich zugängliche Unternehmensdaten, Funktionsadressen und berufliche Kontaktdaten potenzieller Geschäftspartner. Die Verarbeitung dient der Kontaktaufnahme, Angebotsunterbreitung und Bewertung potenzieller Geschäftsbeziehungen. Grundlage ist das berechtigte Interesse an Direktwerbung im B2B Sektor.

h. Bewerbungen

Falls Bewerbungsprozesse über die Website oder per E-Mail abgewickelt werden, verarbeitet Hyptime die bereitgestellten Bewerbungsdaten wie Lebenslauf, Kontaktdaten, Zeugnisse, berufliche Erfahrungen und Notizen aus Interviews. Die Verarbeitung dient der Entscheidung über eine mögliche Anstellung. Nach Abschluss des Verfahrens werden Bewerberdaten gemäß gesetzlicher Fristen gelöscht.

i. Sicherheitsmaßnahmen und Missbrauchserkennung

Zur Sicherstellung der IT Sicherheit und zur Abwehr von Angriffen werden technische Protokolle, IP-Adressen, Login-Versuche, Fehlerprotokolle und sicherheitsrelevante

Ereignisse verarbeitet. Diese Verarbeitung dient der Verhinderung unbefugter Zugriffe, der Aufklärung von Vorfällen und der Integrität der Systeme.

j. Analyse, Statistik und Reichweitenmessung

Um die Plattform, die Website und die Nutzung der Dienste zu verbessern, verarbeitet Hyptime aggregierte Nutzungsdaten, technische Daten, Interaktionsdaten sowie pseudonymisierte Cookies oder Tracking-Informationen. Die Analyse dient Produktoptimierung, Fehlersuche und strategischer Weiterentwicklung.

k. Cookies und vergleichbare Technologien

Zur Bereitstellung der Website und bestimmter Funktionen werden Cookies und ähnliche Technologien eingesetzt. Dazu gehören essenzielle Cookies für Login und Sicherheitsfunktionen sowie optionale Cookies für Analyse und Marketing. Nutzer können in den Cookie Einstellungen individuell entscheiden, welche Kategorien sie zulassen.

l. Verarbeitung von Unternehmensdaten, Mitarbeiterdaten und geschützten Inhalten innerhalb des Kundenkontos

Im Rahmen der Nutzung unserer Plattform, insbesondere der E-Rechnungs- und API-Module, können Kunden personenbezogene Daten ihrer eigenen Beschäftigten, Geschäftspartner, Endkunden und Rechnungsempfänger in das System eingeben. Für die Rechtmäßigkeit dieser Eingaben, die Einholung erforderlicher Einwilligungen der Betroffenen (z. B. der eigenen Endkunden des Nutzers) sowie die inhaltliche Richtigkeit ist ausschließlich der Kunde verantwortlich (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO). Hyptime führt keine inhaltliche Vorabkontrolle, Überwachung oder rechtliche Prüfung der vom Kunden hochgeladenen oder generierten Daten (wie Rechnungsadressen oder Kaufhistorien von Dritten) durch. Wir verarbeiten diese Daten ausschließlich nach den dokumentierten Weisungen des Kunden auf Grundlage eines separat abzuschließenden Auftragsverarbeitungsvertrags (AVV).

Die Plattform wendet modernste kryptografische Verfahren an, um sensible personenbezogene Daten (wie z. B. E-Mail-Adressen) zu schützen. Hierzu zählen pseudonymisierte Hash-Verfahren (z. B. SHA-256) sowie starke Verschlüsselungen (z. B. AES-256-GCM). Eine vollumfängliche, standardmäßige Verschlüsselung aller weiteren Datenbankinhalte oder hochgeladenen Dateien erfolgt nicht, es sei denn, dies wird von Hyptime aus Sicherheitsgründen als zwingend erforderlich erachtet oder vom Kunden als Zusatzleistung ausdrücklich vertraglich beauftragt.

Von Kunden hochgeladene Dateien (Dokumente, Bilder, Anhänge) werden standardmäßig unverschlüsselt gespeichert, es sei denn, dies wird ausdrücklich vertraglich abweichend vereinbart. Sobald der Kunde Daten aus der Plattform exportiert oder über Schnittstellen (API) überträgt, liegt die weitere Sicherung dieser Daten ausschließlich in seinem Verantwortungsbereich.

5. Rechtsgrundlagen der Verarbeitung

a. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung)

Wenn Nutzer freiwillig in bestimmte Verarbeitungen einwilligen, erfolgt die Verarbeitung

auf Grundlage dieser Einwilligung. Dies betrifft insbesondere die Nutzung der Standortfunktion der digitalen Stempeluhr und Zeiterfassungsterminal. Standortdaten werden nur erfasst, wenn der jeweilige Nutzer der Standortfreigabe innerhalb des Browsers oder der App ausdrücklich zugestimmt hat. Die Genauigkeit der Standortdaten kann je nach Endgerät, Browser, Netzbetreiber und Umgebung variieren. Der Kunde entscheidet im Rahmen seiner Verantwortlichkeit, ob die Standortfunktion in seinem Unternehmen genutzt wird. Die technische Einwilligung der einzelnen Nutzer bleibt davon unberührt und ist zwingend erforderlich. Eine Verarbeitung ohne Einwilligung findet nicht statt.

b. Art. 6 Abs. 1 lit. b DSGVO (Vertrag und vorvertragliche Maßnahmen)

Die Verarbeitung ist erforderlich, um den Vertrag mit Kunden zu erfüllen oder um vorvertragliche Maßnahmen durchzuführen. Hierzu gehören Registrierung, Bereitstellung der Plattform, Abrechnung, Nutzerverwaltung, Bereitstellung von Funktionen der Human-Resources-Module sowie Datenverarbeitungen, die notwendig sind, um die Dienstleistungen ordnungsgemäß bereitstellen zu können.

c. Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)

Wir verarbeiten bestimmte Daten zur Wahrung berechtigter Interessen, sofern die Interessen oder Grundrechte der betroffenen Personen nicht überwiegen. Dazu zählen Sicherheitsmaßnahmen wie Missbrauchserkennung, Schutz der Infrastruktur, Logging technischer Vorgänge, statistische Auswertungen in anonymisierter Form sowie betriebliche Optimierungen des Dienstes. Kunden können ebenfalls berechnete Interessen an der Nutzung der Plattform haben, insbesondere im Rahmen der Personalverwaltung.

d. Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Verpflichtung)

Es werden Daten verarbeitet, wenn dies zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist. Dies kann steuerliche Aufbewahrungspflichten, handelsrechtliche Vorschriften, arbeitsrechtliche Pflichten des Kunden oder Dokumentationsanforderungen betreffen.

e. TTDSG (Deutschland) bei Cookies und Tracking

Soweit Cookies oder ähnliche Technologien auf Endgeräten gespeichert oder ausgelesen werden, richtet sich dies nach dem TTDSG. Erforderliche Cookies dürfen ohne Einwilligung eingesetzt werden, während nicht erforderliche Cookies, etwa zu Analyse- oder Marketingzwecken, nur mit Einwilligung genutzt werden.

6. Datenverarbeitung im Rahmen der Plattformnutzung

a. Verarbeitete Daten der Nutzerkonten

Bei der Erstellung und Nutzung von Nutzerkonten verarbeiten wir die notwendigen personenbezogenen Daten der einzelnen Nutzer. Dazu gehören Name, E Mail Adresse, Passwort Hash, Rollen und Zuordnungen innerhalb des Unternehmens. In optionalen HR

Modulen können zusätzliche Daten verarbeitet werden, etwa Bankverbindungen, Adressen, Geburtsdaten oder andere personalbezogene Informationen, die der Kunde im Rahmen seiner Nutzung eingibt. Sämtliche Daten werden ausschließlich zur Bereitstellung der vertraglich vereinbarten Funktionen verarbeitet.

b. Teamverwaltung, Rollen und Berechtigungen

Die Plattform unterstützt die Verwaltung von Teams und Rollen. Der Kunde legt fest, welche Nutzer welche Berechtigungen erhalten. Wir verarbeiten die entsprechenden Daten zur Bereitstellung der Rollenlogik sowie zur Kontrolle von Zugriffsrechten. Der Kunde bleibt Verantwortlicher für alle personenbezogenen Daten, die er für die Verwaltung seiner Mitarbeiter verarbeitet.

c. Verarbeitete Dokumente und Dateien im Dokumentenspeicher

Dokumente, Dateien und Medien, die der Kunde im Dokumentenspeicher ablegt, werden verarbeitet, um die jeweiligen Funktionen der Plattform bereitzustellen. Persönliche Dokumente, die sensible Daten enthalten können, werden standardmäßig nicht verschlüsselt, sofern nichts anderes vereinbart ist. Auf Wunsch oder auf Grundlage individueller Vertragsbedingungen kann eine zusätzliche Verschlüsselung der gespeicherten Dateien erfolgen.

d. Aktivitätsdaten, Logs und Audit Trails

Zur Sicherheit, Fehlerdiagnose und Nachvollziehbarkeit bestimmter Aktionen werden Aktivitätsdaten und technische Logs verarbeitet. Dazu zählen Zeitstempel, Nutzeraktionen innerhalb der Plattform, Systemereignisse sowie Sicherheitsprotokolle. Diese Daten dienen ausschließlich der Bereitstellung, Stabilität und sicheren Nutzung des Dienstes.

e. Backup, Restore und Archivierung

Wir erstellen regelmäßige Backups der Daten, um die Betriebssicherheit und die Integrität der Plattform zu sichern. Backups werden verschlüsselt gespeichert. Die Backups dienen ausschließlich der Wiederherstellung und nicht operativen Zwecken. Der Kunde hat keinen direkten Zugriff auf System Backups, kann jedoch Daten innerhalb der Plattform exportieren. Archivierungsfunktionen ermöglichen es dem Kunden, bestimmte Daten innerhalb seines Kontos aus dem aktiven Betrieb zu entfernen, ohne sie sofort zu löschen.

f. Datenlöschung und Speicherfristen

Daten werden gelöscht, sobald sie für den jeweiligen Zweck nicht mehr erforderlich sind, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Der Kunde entscheidet selbst, wann er Stammdaten seiner Nutzer löscht. Nach Vertragsende werden Daten innerhalb der vereinbarten Fristen gelöscht. Der Kunde erhält vor der endgültigen Löschung die Möglichkeit, Daten zu exportieren, sofern keine gesetzlichen Hindernisse bestehen.

g. Mandantentrennung und Verschlüsselung

Die Plattform ist mandantenfähig aufgebaut. Kundendaten werden logisch voneinander getrennt. Bestimmte personenbezogene Daten, insbesondere sensible HR Daten wie

Bankverbindungen, Adressdaten oder Steuerdaten, werden mit AES 256 GCM verschlüsselt gespeichert. Dokumente und Medien werden standardmäßig nicht verschlüsselt, können jedoch auf Wunsch des Kunden oder aufgrund individueller Vereinbarungen ebenfalls verschlüsselt abgelegt werden. Daten im Backup sind grundsätzlich verschlüsselt. Daten im Transit werden mittels aktueller Transportverschlüsselung übermittelt.

7. Zahlungsdaten

a. Zahlungsarten und gespeicherte Daten

Bei der Nutzung kostenpflichtiger Leistungen verarbeiten wir die Daten, die zur Zahlungsabwicklung notwendig sind. Die konkret verarbeiteten Daten hängen von der Zahlungsart ab, die Ihnen für Ihr gewähltes Produkt oder Tarifmodell zur Verfügung gestellt und von Ihnen ausgewählt wird. Dazu gehören Rechnungsdaten, Firmenname, Anschrift, E-Mail-Adresse für Rechnungen sowie technische Zahlungsinformationen. Bei der Nutzung von Kreditkarten oder digitalen Wallets (Apple Pay, Google Pay, Stripe Link) werden Ihre vollständigen Kreditkartendaten nicht bei uns gespeichert. Wir speichern zur Rechnungszuordnung und für zukünftige Abbuchungen lediglich ein verschlüsseltes, gerätespezifisches Zahlungs-Token (z. B. DPAN bei Apple Pay) sowie die letzten vier Ziffern der Karte, welche wir von unserem Zahlungsdienstleister erhalten.

b. Übermittlung an Zahlungsdienstleister

Zur Durchführung von automatisierten Zahlungen (Kreditkarte, Wallets, SEPA) nutzen wir den Zahlungsdienstleister Stripe, Inc. (bzw. deren europäische Tochtergesellschaften). Wir übermitteln die für die Zahlung notwendigen Transaktionsdaten an Stripe. Die Zahlungsdienstleister verarbeiten die Daten in eigener Verantwortung, soweit dies für die Abwicklung der Zahlung erforderlich ist. Bei der Nutzung von Apple Pay oder Google Pay gelten zusätzlich die Datenschutzbestimmungen der jeweiligen Anbieter (Apple Inc. / Google LLC). Wir erhalten von Stripe ausschließlich Bestätigungen über erfolgreiche oder fehlgeschlagene Transaktionen.

c. Identitäts und Betrugsprüfung

Je nach Zahlungsart kann der Zahlungsdienstleister (insbesondere Stripe) zusätzliche Prüfungen durchführen, etwa Identitätsprüfungen, Risikobewertungen oder Betrugsprävention durch Geräteerkennung (Device Fingerprinting). Diese Prüfungen erfolgen im strengen Verantwortungsbereich des Zahlungsdienstleisters. Wir erhalten keine detaillierten Prüfergebnisse, sondern lediglich die Freigabe oder Ablehnung der Transaktion.

d. Löschfristen für Zahlungsdaten

Zahlungsrelevante Daten (Rechnungen, Transaktions-Logs, Zahlungstokens) speichern wir nur so lange, wie dies für die Erfüllung der laufenden Verträge sowie gesetzlicher Aufbewahrungspflichten notwendig ist. In der Regel handelt es sich um handels- und steuerrechtliche Aufbewahrungsfristen von bis zu zehn Jahren. Daten, die nicht solchen Pflichten unterliegen, werden gelöscht, sobald sie zur Zahlungsabwicklung nicht mehr benötigt werden oder das erteilte SEPA- bzw. Zahlungs-Mandat widerrufen wurde.

8. Cookies und Tracking Technologien

a. Technisch notwendige Cookies

Wir verwenden technisch notwendige Cookies, um den sicheren und stabilen Betrieb der Website und Plattform zu gewährleisten. Dazu gehören Funktionen wie Login Verwaltung, Sitzungserhaltung und sicherheitsrelevante Schutzmechanismen. Diese Cookies sind für die Nutzung unserer Dienste zwingend erforderlich und können nicht deaktiviert werden. Die Verarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit § 25 Abs. 2 TTDSG.

b. Funktionale Cookies

Funktionale Cookies ermöglichen Komfortfunktionen wie Sprachauswahl, Systemeinstellungen oder die Speicherung bestimmter Nutzervorgaben. Diese Cookies verarbeiten anonymisierte oder pseudonymisierte Daten und basieren auf Art. 6 Abs. 1 lit. a DSGVO, sofern sie nicht zwingend technisch erforderlich sind. Nutzer können diese Cookies jederzeit über die Cookie Einstellungen widerrufen.

c. Statistik und Analyse

Für die Analyse des Nutzerverhaltens können wir datenschutzkonforme Tracking Werkzeuge einsetzen, etwa Google Analytics oder alternative Lösungen wie Matomo. Die Analyse dient der Optimierung unserer Plattform und der Verbesserung der Systemstabilität. Je nach eingesetztem Anbieter erfolgt die Verarbeitung auf Grundlage von Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit § 25 Abs. 1 TTDSG. Die Verarbeitung erfolgt in pseudonymisierter Form. Eine Übermittlung in Drittländer ist möglich und richtet sich nach den jeweils gültigen Schutzmechanismen wie Standardvertragsklauseln.

d. Marketing und Personalisierungs Cookies

Marketing und personalisierte Cookies dienen dazu, Nutzern interessenbezogene Inhalte und Angebote anzuzeigen. Diese Technologien können auch von Drittanbietern stammen. Die Verarbeitung basiert ausschließlich auf Einwilligung. Ohne Zustimmung werden keine Marketing Cookies gesetzt und keine nutzerbezogenen Profile erstellt. Nutzer können die Einwilligung jederzeit widerrufen.

e. Cookie Einstellungen und Widerruf

Nutzer können sämtliche nicht notwendigen Cookies über das Cookie Management Tool auf unserer Website verwalten und ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Bereits gesetzte Cookies können zudem über die Einstellungen des Browsers gelöscht werden. Die Auswahl wird gespeichert, bis sie durch den Nutzer erneut angepasst wird.

f. Kontaktformular / Rückruf-Service

Wenn Sie uns über ein Kontaktformular oder unseren Rückruf-Service erreichen, verarbeiten wir die von Ihnen eingegebenen Daten (z. B. Name, Adresse, E-Mail-Adresse, Telefonnummer, Nachricht). Zusätzlich werden aus technischen Gründen automatisch

Server-Logdaten erfasst, darunter IP-Adresse, Zeitpunkt der Anfrage und technische Metadaten.

Die Verarbeitung erfolgt ausschließlich zur Bearbeitung Ihrer Anfrage und auf Grundlage Ihrer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

Die Übermittlung kann über interne Systeme sowie externe Auftragsverarbeiter erfolgen (z. B. E-Mail-Provider, CRM-Systeme). Eine Weitergabe an Dritte erfolgt nicht ohne Ihre Zustimmung.

Die Daten speichern wir, bis Ihre Anfrage abschließend bearbeitet wurde oder Sie Ihre Einwilligung widerrufen. Logdaten werden gemäß den technischen Erfordernissen automatisiert nach kurzer Zeit gelöscht. Gesetzliche Aufbewahrungsfristen bleiben unberührt.

9. Analyse- und Marketing-Tools

a. Google Analytics

Wir setzen Google Analytics ein, sofern der Nutzer dafür eine Einwilligung erteilt hat. Google Analytics ist ein Webanalyse-Dienst der Google Ireland Limited. Das Tool verwendet Cookies oder vergleichbare Technologien, um das Verhalten der Besucher auszuwerten und Berichte über die Nutzung unserer Website zu erstellen. Die Erfassung erfolgt pseudonymisiert. Eine Übermittlung in die USA kann stattfinden und basiert auf Standardvertragsklauseln. Die Verarbeitung erfolgt ausschließlich auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit § 25 Abs. 1 TTDSG. Nutzer können ihre Einwilligung jederzeit widerrufen. Google speichert die Daten entsprechend der von uns definierten Aufbewahrungsfristen.

b. Google Tag Manager

Falls wir den Google Tag Manager einsetzen, wird dies ausschließlich zur Verwaltung von Tracking- und Marketing-Skripten genutzt. Der Tag Manager selbst verarbeitet keine personenbezogenen Daten. Er lädt lediglich weitere Dienste nach, deren Einsatz von der Einwilligung des Nutzers abhängt. Eine Aktivierung erfolgt nur, wenn im Cookie Banner die entsprechende Zustimmung vorliegt. Die Rechtsgrundlage hängt somit von den Diensten ab, die über den Tag Manager eingebunden werden.

c. Newsletter-Tracking

Wenn Nutzer unseren Newsletter abonnieren, kann eine Erfolgsmessung erfolgen. Dazu gehören Informationen darüber, ob eine E-Mail geöffnet wurde sowie welche Links angeklickt wurden. Die Daten dienen ausschließlich zur Verbesserung unserer Inhalte. Die Verarbeitung basiert auf Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO. Das Tracking erfolgt nur, wenn im Rahmen der Newsletter-Anmeldung ausdrücklich zugestimmt wurde. Nutzer können das Tracking durch Abmeldung vom Newsletter oder Änderung ihrer Cookie Einstellungen beenden.

d. Opt-Out-Mechanismen

Nutzer können das Tracking jederzeit deaktivieren. Dafür stehen die folgenden Wege zur Verfügung:

Widerruf der Einwilligung über das Cookie-Banner

Browser-Einstellungen zur Blockierung von Cookies oder Tracking-Technologien

Opt-Out-Cookies der jeweiligen Anbieter

Deaktivierung der Dienste über die individuellen Datenschutz-Links der Tools

Ein Widerruf wirkt sich nicht auf die Rechtmäßigkeit der vorherigen Verarbeitung aus.

Jede Entscheidung wird technisch umgesetzt und gilt für zukünftige Websitebesuche.

e. HR-Expertise (Newsletter)

Wenn Sie sich für unseren HR-Expertise-Newsletter anmelden, verarbeiten wir die von Ihnen angegebenen Daten ausschließlich zum Versand des Newsletters und zur Bereitstellung damit verbundener Inhalte. Die Verarbeitung erfolgt auf Grundlage Ihrer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO.

Für die Anmeldung verwenden wir das Double-Opt-In-Verfahren, um sicherzustellen, dass die Anmeldung tatsächlich durch Sie erfolgt ist.

Im Rahmen der Nutzung des Newsletters können folgende Daten verarbeitet werden: Name, Kontaktdaten, Unternehmensinformationen sowie Interaktionsdaten mit dem Newsletter. Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Den Abmelde-Link finden Sie in jeder E-Mail. Alternativ können Sie Ihre Abmeldung per E-Mail mitteilen.

Nach einem Widerruf wird Ihre E-Mail-Adresse aus der Versandliste entfernt und in einer internen Sperrliste gespeichert, um sicherzustellen, dass kein weiterer Newsletter an Sie versendet wird. Diese Speicherung erfolgt auf Grundlage unseres berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO, um unzulässige Zusendungen zu verhindern. Die Adresse wird ausschließlich für diesen Zweck genutzt.

f. Kundenakquise / B2B-Direktwerbung

Im Rahmen unserer vertrieblichen Aktivitäten verarbeiten wir geschäftliche Kontaktinformationen von Unternehmen und deren Ansprechpartnern. Diese Daten stammen entweder aus öffentlich zugänglichen Quellen oder aus Recherchen durch unser Vertriebsteam. Die Verarbeitung erfolgt zur Kontaktaufnahme, zur Informationsbereitstellung und zur Bewerbung unserer Produkte und Dienstleistungen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO, basierend auf unserem berechtigten Interesse an Direktwerbung im B2B-Bereich.

Der Kontakt kann per E-Mail, Telefon oder postalisch erfolgen. Sie können der Nutzung Ihrer Daten für Direktwerbung jederzeit widersprechen. Jeder von uns versendete Werbe- oder Informationskontakt enthält einen entsprechenden Opt-Out-Hinweis. Alternativ können Sie Ihren Widerspruch per E-Mail übermitteln.

Nach einem Widerspruch speichern wir die betreffende E-Mail-Adresse oder Telefonnummer ausschließlich in einer internen Sperrliste, um sicherzustellen, dass zukünftig keine weitere werbliche Ansprache erfolgt. Eine Löschung der Daten erfolgt

nicht, da ansonsten eine erneute versehentliche Kontaktaufnahme nicht ausgeschlossen werden kann. Die Verarbeitung in der Sperrliste erfolgt nur zu diesem Zweck und auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit Art. 21 DSGVO.

Wir speichern Akquise-Daten nur so lange, wie der Zweck der Kontaktaufnahme besteht. Entfällt dieser Zweck, werden die Daten gelöscht oder – im Fall eines Widerspruchs – dauerhaft gesperrt.

10. Einbindung von Diensten Dritter

a. Google Maps

Wenn Google Maps eingebunden ist, werden beim Aufruf der Seite Karteninhalte von Google geladen. Dabei überträgt Ihr Browser technische Daten wie IP-Adresse, Geräteinformationen und ggf. Standortdaten an Google. Google kann diese Daten zu eigenen Zwecken verarbeiten. Rechtsgrundlage ist Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO, sofern Maps erst nach Zustimmung geladen wird. Ohne Einwilligung darf Google Maps nicht technisch automatisch eingebunden werden.

b. YouTube

Beim Abspielen eingebetteter YouTube-Videos werden technische Daten (IP-Adresse, Geräteinformationen, ggf. Cookies) an Google übermittelt. Wenn möglich, wird der erweiterte Datenschutzmodus („privacy-enhanced mode“) verwendet. Die Verarbeitung basiert auf Ihrer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Ohne Einwilligung dürfen Videos nicht automatisch starten oder geladen werden.

c. reCAPTCHA

reCAPTCHA prüft, ob Aktionen auf der Website durch Menschen oder durch automatisierte Systeme erfolgen. Dafür analysiert Google verschiedene technische Daten wie Mausbewegungen, IP-Adresse, Browser- und Geräteinformationen. Die Nutzung erfolgt auf Grundlage unseres berechtigten Interesses an der Sicherung unserer Systeme gemäß Art. 6 Abs. 1 lit. f DSGVO. Falls reCAPTCHA erst nach Zustimmung geladen wird, ist Art. 6 Abs. 1 lit. a DSGVO einschlägig.

d. CDN-Dienste (Cloudflare oder andere)

Ein Content Delivery Network (CDN) beschleunigt die Auslieferung der Website oder der Plattform. Beim Abruf von Inhalten werden technische Daten (IP-Adresse, Zugriffszeit, angeforderte Ressourcen) über die Server des CDN-Anbieters geleitet. Anbieter wie Cloudflare verarbeiten diese Daten, um Angriffe abzuwehren und die Übertragung zu optimieren. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an sicherem und effizientem Betrieb). Wenn das CDN als Sicherheitsdienst fungiert, ist dies technisch zwingend erforderlich.

e. Weitere Drittanbieter

Wenn zusätzliche externe Dienste eingebunden werden (z. B. Webfonts, Captcha-Dienste,

Support-Chat-Widgets, Kartendienste, API-Dienste), werden die dabei verarbeiteten Daten nur im für den Betrieb notwendigen Umfang an die jeweiligen Anbieter übermittelt. Die konkrete Verarbeitung, Rechtsgrundlage und Speicherfristen werden – falls zutreffend – in den entsprechenden Abschnitten dieser Datenschutzerklärung erläutert oder auf gesonderten Unterseiten beschrieben.

11. Hosting

a. Hostinganbieter (Strato)

Die Plattform und die Website werden auf Servern der Strato AG betrieben. Strato stellt die technische Infrastruktur, Rechenzentrumsumgebung, Netzwerkanbindung und Sicherheitsmechanismen bereit. Personenbezogene Daten, die über die Plattform verarbeitet werden, werden auf den Systemen von Strato gespeichert und verarbeitet.

b. Logfiles

Strato protokolliert automatisiert Server-Logfiles. Dazu gehören die IP-Adresse des zugreifenden Systems, Datum und Uhrzeit der Anfrage, aufgerufene Datei, Menge der übertragenen Daten, Herkunfts-URL (Referrer), Browsertyp und -version sowie Betriebssystem. Diese Daten sind technisch notwendig, um Angriffe zu erkennen, Störungen zu beheben und die Stabilität des Betriebs sicherzustellen. Die Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Logfiles werden nach den vom Hostinganbieter definierten Fristen automatisch gelöscht (in der Regel 7 Tage, abhängig vom Strato-Setup).

c. Unterauftragnehmer

Strato kann für bestimmte Prozesse eigene Unterauftragnehmer einsetzen (z. B. für Rechenzentrumsbetrieb, Netzwerk, physische Sicherheit). Diese Unterauftragnehmer handeln ausschließlich nach Weisung von Strato. Eine darüber hinausgehende Weitergabe der Daten erfolgt nicht. Eine aktuelle Liste der von Strato eingesetzten Subunternehmer kann beim Hostinganbieter eingesehen oder beim Verantwortlichen angefragt werden.

d. Geografische Datenlokation

Die Daten werden ausschließlich in Rechenzentren innerhalb Deutschlands gespeichert. Strato betreibt zertifizierte Rechenzentren in Berlin und Karlsruhe. Es findet keine Übermittlung personenbezogener Daten in Drittländer statt, sofern keine zusätzlichen externen Dienste ausdrücklich eingebunden werden.

e. AVV mit Hostingpartnern

Mit Strato besteht ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO. Dieser regelt technische und organisatorische Maßnahmen, Vertraulichkeitspflichten, Subunternehmer-Einsatz und Kontrollrechte. Die Verarbeitung erfolgt ausschließlich nach dokumentierten Weisungen des Verantwortlichen.

12. Auftragsverarbeiter und Unterauftragsverarbeiter

a. Kategorien von Auftragsverarbeitern

Für den Betrieb der Plattform werden externe Dienstleister eingesetzt, die personenbezogene Daten ausschließlich nach Weisung verarbeiten. Zu diesen Dienstleistern gehören:

- Hosting- und Infrastrukturprovider
- E-Mail- und Kommunikationsdienstleister
- Support- und Ticketing-Systeme
- Backup- und Archivierungsdienste
- Zahlungsdienstleister, soweit diese im Rahmen der Auftragsverarbeitung agieren
- Analyse- und Sicherheitsdienste (z. B. DDoS-Schutz)

Alle Auftragsverarbeiter sind vertraglich nach Art. 28 DSGVO verpflichtet, angemessene technische und organisatorische Maßnahmen einzuhalten.

b. Subunternehmerliste

Eine Liste der eingesetzten Subunternehmer (inklusive Hostinganbieter, technische Dienstleister und sonstige Infrastrukturpartner) wird bereitgestellt und bei Änderungen aktualisiert. Kunden können diese Liste anfordern oder über ein entsprechendes Systemmodul einsehen. Neue Subunternehmer werden mindestens 30 Tage vor Einsatz angekündigt, sofern vertraglich vereinbart.

c. Prüf- und Kontrollrechte

Kunden haben nach Art. 28 Abs. 3 lit. h DSGVO das Recht, die Einhaltung der vereinbarten Datenschutzmaßnahmen zu prüfen. Dies umfasst:

- Einsicht in relevante Auditberichte und Zertifizierungen (z. B. ISO 27001)
- technische und organisatorische Maßnahmen (TOMs)
- Informationen zu Sicherheitsstandards und Prozessen

Physische Audits vor Ort sind nur nach vorheriger Abstimmung möglich und richten sich nach den Bedingungen der jeweiligen Unterauftragnehmer.

d. Datenübermittlung in Drittstaaten

Eine Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWR findet nicht statt, es sei denn, einzelne Dienste werden ausdrücklich genutzt, die technisch in Drittländern betrieben werden. In diesem Fall erfolgt die Übermittlung nur, wenn geeignete Garantien nach Art. 44 ff. DSGVO bestehen.

e. Garantien (Standardvertragsklauseln etc.)

Falls Dienstleister außerhalb der EU eingesetzt werden, erfolgt die Übermittlung ausschließlich auf Basis geeigneter Garantien:

- EU-Standardvertragsklauseln (SCC)
- anerkannte Zertifizierungen
- Angemessenheitsbeschluss der EU-Kommission
- zusätzliche Schutzmaßnahmen wie Verschlüsselung und Minimierung

Sind diese Voraussetzungen nicht erfüllt, werden entsprechende Dienste nicht genutzt.

13. Datenübermittlung an Dritte

a. Zweckgebundene Übermittlung

Personenbezogene Daten werden nur dann an Dritte übermittelt, wenn dies für die Erfüllung vertraglicher Pflichten, die technische Bereitstellung der Plattform oder gesetzliche Anforderungen notwendig ist. Eine Weitergabe erfolgt ausschließlich zweckgebunden und nach den Vorgaben der DSGVO.

b. Übermittlung an Zahlungsanbieter

Für die Zahlungsabwicklung werden Daten an Zahlungsdienstleister übermittelt. Dazu gehören z. B. Rechnungsdaten, Kundennummern oder Transaktionsinformationen. Die Übermittlung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO, da sie für die Durchführung des Vertrags erforderlich ist.

c. Übermittlung an Behörden

Eine Weitergabe an Behörden erfolgt nur, wenn eine gesetzliche Verpflichtung besteht oder eine behördliche Anordnung vorliegt. Rechtsgrundlage ist Art. 6 Abs. 1 lit. c DSGVO.

d. Kein Verkauf oder Vermietung von Daten

Es findet keine Weitergabe personenbezogener Daten zu kommerziellen Zwecken statt. Daten werden nicht verkauft, nicht vermietet und nicht für externe Werbenetzwerke bereitgestellt.

e. Forderungsdurchsetzung und Inkasso

Befindet sich der Kunde mit Zahlungen in Verzug und führt das automatisierte Mahnwesen von Hyptime nicht zum Zahlungsausgleich, behalten wir uns vor, die zur Forderungsdurchsetzung erforderlichen personenbezogenen Daten (Stammdaten, Rechnungsdaten, Kommunikationsverlauf, Logfiles zum Nutzungsnachweis) an Rechtsanwälte, Inkassounternehmen sowie Auskunftsteilen zu übermitteln. Die Verarbeitung und Übermittlung erfolgt in diesem Fall auf Grundlage von Art. 6 Abs. 1 lit. b

und lit. f DSGVO zur Wahrung unseres berechtigten Interesses an der Durchsetzung unserer vertraglichen und rechtlichen Ansprüche.

f. Automatisierter Datenexport an externe Buchhaltungssysteme und Steuerberater

Nutzt der Kunde Funktionen zum automatisierten oder manuellen Export von Rechnungs- und Finanzdaten in externe Systeme (z. B. DATEV-Export, SAP-Schnittstellen oder andere ERP- und Buchhaltungssoftware), werden die ausgewählten Datenpakete an die vom Kunden konfigurierten Schnittstellen oder Empfänger (z. B. den externen Steuerberater) übermittelt. Diese Übermittlung erfolgt ausschließlich auf ausdrückliche, dokumentierte Anweisung des Kunden im Rahmen der Vertragserfüllung (Art. 6 Abs. 1 lit. b in Verbindung mit Art. 28 DSGVO). Sobald die personenbezogenen und steuerlich relevanten Daten die Infrastruktur von Hyptime über die Schnittstelle verlassen, liegt die alleinige datenschutzrechtliche Verantwortung für die sichere Übertragung und weitere rechtskonforme Verarbeitung beim Kunden bzw. beim jeweiligen Drittanbieter.

g. Nutzung externer Speicheranbieter durch den Kunden (Bring Your Own Storage)

Entscheidet sich der Kunde dafür, eigene Cloud-Speicher oder S3-kompatible Speicherlösungen von Drittanbietern (z. B. Amazon Web Services, Google Cloud) in die Plattform zu integrieren, werden die betroffenen Dateien (z. B. Dokumente, Rechnungen, Anhänge) direkt an die Systeme dieses Drittanbieters übermittelt und dort gespeichert. Hyptime speichert in diesem Fall auf eigenen Servern lediglich die strukturellen Metadaten (z. B. Dateinamen, Zeitstempel, Datenbankverweise) zur Aufrechterhaltung der Software-Funktionalität. Die datenschutzrechtliche Verantwortung für die Speicherung der Inhalte auf dem Fremdsystem sowie der Abschluss etwaiger erforderlicher Auftragsverarbeitungsverträge (AVV) mit dem jeweiligen Speicher-Drittanbieter liegt bei dieser Konfiguration ausschließlich und vollumfänglich beim Kunden.

Temporäre Fallback-Speicherung: Schlägt die Übertragung an den externen Speicher des Kunden fehl (z. B. aufgrund technischer Ausfälle beim Drittanbieter oder fehlgeschlagener Authentifizierung), werden die betroffenen Dokumente und die darin enthaltenen personenbezogenen Daten zur Vermeidung von Datenverlusten temporär auf den eigenen, gesicherten Servern von Hyptime zwischengespeichert (Notfall-Puffer). Diese Zwischenspeicherung erfolgt auf Grundlage unseres berechtigten Interesses an der Aufrechterhaltung der Systemstabilität, der Abwicklung laufender Vertragsprozesse (Art. 6 Abs. 1 lit. f DSGVO) sowie zwingend im Rahmen der Auftragsverarbeitung. Sobald die Verbindung zum Fremdsystem des Kunden wiederhergestellt ist, werden die Daten synchronisiert und die temporären Kopien auf unseren Systemen automatisiert gelöscht.

14. Internationale Datenübermittlung

a. EU / EWR

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Eine Übermittlung in

andere Staaten findet nur statt, wenn dies für die Leistungserbringung erforderlich ist oder gesetzlich vorgeschrieben ist.

b. Drittstaatentransfer

Wenn Dienstleister oder technische Systeme außerhalb des EU/EWR eingesetzt werden, erfolgt die Übermittlung personenbezogener Daten nur unter Beachtung der DSGVO. Daten werden ausschließlich dann in Drittländer übertragen, wenn ein angemessenes Datenschutzniveau gewährleistet ist.

c. Rechtsgrundlagen für Übermittlung in die USA

Bei der Übermittlung in die USA wird geprüft, ob der Empfänger unter dem „EU-US Data Privacy Framework“ zertifiziert ist. Ist dies nicht der Fall, erfolgt die Übermittlung nur auf Grundlage einer anderen gültigen Rechtsgrundlage nach Art. 44 ff. DSGVO.

d. Sicherungsmechanismen (SCC, Art. 46 DSGVO)

Sofern kein Angemessenheitsbeschluss besteht, werden geeignete Garantien eingesetzt. Dazu gehören insbesondere die von der EU-Kommission veröffentlichten Standardvertragsklauseln (SCC), zusätzliche vertragliche, organisatorische oder technische Schutzmaßnahmen und Risikoanalysen gemäß DSGVO.

15. Datensicherheit / Technische und organisatorische Maßnahmen (TOMs)

a. Verschlüsselung (Transport, Ruhe)

Daten werden während der Übertragung per TLS geschützt. Ausgewählte, besonders schutzbedürftige Datensätze (wie z.B. E-Mail-Adressen, Authentifizierungsdaten) werden zusätzlich mit starken kryptografischen Verfahren (Hashing und/oder Verschlüsselung wie AES-256 im Ruhezustand) gesichert. Eine pauschale Verschlüsselung sämtlicher Datenbankinhalte oder hochgeladener Dateien erfolgt nur nach spezifischer vertraglicher Vereinbarung.

b. Zugriffsbeschränkung / Zugriffskontrolle

Der Zugang zur Plattform erfolgt über Benutzerkonten mit individuellen Zugangsdaten. Passwortrichtlinien und Session-Sicherheit reduzieren Missbrauchsrisiken. Zugriff auf produktive Systeme ist nur autorisierten Mitarbeitern des Anbieters möglich, streng nach dem Need-to-Know-Prinzip.

c. Protokollierung und Monitoring

Systemereignisse, sicherheitsrelevante Vorgänge und administrative Aktionen werden protokolliert, um den sicheren Betrieb der Plattform sicherzustellen und Störungen analysieren zu können. Die Protokolle werden nach festen Fristen gelöscht.

d. Physische Sicherheit

Die genutzten Rechenzentren sind durch Zutrittskontrollen, Videoüberwachung, Brandmelde- und Löschsysteeme sowie Redundanzen abgesichert. Der Betrieb erfolgt ausschließlich in professionellen Hochsicherheitsrechenzentren.

e. Backup-Strategie

Regelmäßige Backups sorgen für Wiederherstellbarkeit. Backups werden nach festen Intervallen erstellt und innerhalb der vereinbarten Fristen aufbewahrt. Backups werden verschlüsselt gespeichert.

f. Penetrationstests / Sicherheitsüberprüfungen

Sicherheitsmaßnahmen werden regelmäßig überprüft. Dazu gehören interne Tests, externe Sicherheitsaudits und technische Schwachstellenanalysen, um Risiken früh zu erkennen und zu beheben.

g. Incident Response und Meldeprozesse

Sicherheitsvorfälle werden nach einem standardisierten Verfahren bearbeitet. Falls personenbezogene Daten betroffen sind, erfolgt eine Bewertung der Risiken und, wenn gesetzlich erforderlich, eine Meldung an die zuständige Aufsichtsbehörde sowie an betroffene Personen.

16. Rechte der betroffenen Personen

a. Auskunft

Betroffene Personen können Auskunft darüber verlangen, ob und welche personenbezogenen Daten verarbeitet werden. Dazu gehören Verarbeitungszwecke, Kategorien von Daten, Empfänger, Speicherdauer und Rechte.

b. Berichtigung

Betroffene Personen haben das Recht, unrichtige oder unvollständige personenbezogene Daten berichtigen zu lassen.

c. Löschung

Daten werden auf Wunsch gelöscht, wenn die gesetzlichen Voraussetzungen erfüllt sind. Eine vorzeitige Löschung des Kundenkontos und der zugehörigen Daten kann von Hyptime verweigert werden, solange noch offene Forderungen gegen den Kunden bestehen. Zwingende Ausnahme: Nutzt der Kunde Module zur Erstellung, Verarbeitung oder Archivierung von E-Rechnungen und steuerlich relevanten Dokumenten, unterliegen diese den gesetzlichen Aufbewahrungsfristen (z. B. nach HGB, AO, GoBD, i. d. R. 10 Jahre). Ein vorzeitiger Löschantrag des Kunden für diese revisionssicheren Datenbestände ist während der laufenden gesetzlichen Fristen absolut ausgeschlossen (Art. 17 Abs. 3 lit. b

DSGVO).

d. Einschränkung

Betroffene Personen können die Einschränkung der Verarbeitung verlangen, wenn Daten geprüft werden müssen, die Verarbeitung unrechtmäßig ist oder ein Widerspruch geprüft wird.

e. Widerspruch

Die Verarbeitung kann aus Gründen der besonderen Situation der betroffenen Person widersprochen werden, sofern sie auf berechtigten Interessen basiert. Der Widerspruch gegen Direktwerbung wirkt sofort.

f. Datenübertragbarkeit

Betroffene Personen können verlangen, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Daten, soweit technisch möglich, an einen anderen Verantwortlichen übertragen zu lassen.

g. Widerruf

Erteilte Einwilligungen können jederzeit mit Wirkung für die Zukunft widerrufen werden. Die Verarbeitung bis zum Zeitpunkt des Widerrufs bleibt rechtmäßig.

h. Beschwerderecht bei der Aufsichtsbehörde

Betroffene Personen können sich bei einer Datenschutzaufsichtsbehörde beschweren, wenn sie der Ansicht sind, dass die Verarbeitung personenbezogener Daten gegen Datenschutzrecht verstößt. Zuständig ist die Aufsichtsbehörde des Bundeslands des Wohnsitzes oder die für den Anbieter zuständige Aufsicht.

17. Löschfristen und Speicherdauer

a. Gesetzliche Aufbewahrungsfristen

Personenbezogene Daten werden nur so lange gespeichert, wie es gesetzlich erforderlich ist. Dazu gehören insbesondere steuerrechtliche und handelsrechtliche Aufbewahrungsfristen zwischen sechs und zehn Jahren.

b. Kundendaten

Daten aus der Kundenbeziehung, wie Stammdaten, Kontaktinformationen und Kommunikationsdaten, werden für die Dauer des Vertragsverhältnisses gespeichert. Nach Vertragsende werden sie gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten bestehen oder ein anderes berechtigtes Interesse überwiegt.

c. Vertragsdaten

Daten, die für die Abwicklung von Verträgen notwendig sind, werden entsprechend der

gesetzlichen Pflichten gespeichert. Dazu zählen Rechnungen, Zahlungsdaten, Buchungsunterlagen und relevante Korrespondenz.

d. Plattformdaten und E-Rechnungs-Archivierung

Daten, die im Rahmen der Nutzung der Plattform entstehen (z. B. HR-Daten, Projektdaten und Konfigurationen), werden für die Dauer der Nutzung gespeichert und nach Beendigung des Vertrags gelöscht oder anonymisiert.

Sonderregelung für Rechnungsdaten: Rechnungen, Quittungen und E-Rechnungen, die der Kunde über die Plattform erstellt, versendet oder empfängt, werden in einem revisionssicheren Format gespeichert. Hyptime fungiert hierbei als technischer Dienstleister zur Erfüllung der gesetzlichen Aufbewahrungspflichten des Kunden (GoBD). Diese Dokumente werden von Hyptime für die gesetzlich vorgeschriebene Dauer (i. d. R. 10 Jahre zum Jahresende) aufbewahrt und vor vorzeitiger Löschung geschützt, selbst wenn das aktive Vertragsverhältnis des Kunden vorher endet.

e. Logfiles

Server- und Systemlogfiles werden für Sicherheits- und Stabilitätszwecke verarbeitet. Die reguläre Speicherdauer liegt in der Regel zwischen 7 und 90 Tagen. Eine darüber hinausgehende Speicherung erfolgt, sofern dies zur Aufklärung von sicherheitsrelevanten Vorfällen, zur Abwehr von Betrugsversuchen oder zur Beweisführung bei rechtlichen Auseinandersetzungen (insbesondere bei Zahlungsstreitigkeiten oder unberechtigten Rücklastschriften) erforderlich ist. In diesen Fällen werden die relevanten Logfiles bis zur endgültigen Klärung des Vorfalls aufbewahrt (Art. 6 Abs. 1 lit. f DSGVO).

f. Backups

Backups werden in zyklischen Intervallen erstellt und im Rahmen der Backupstrategie für begrenzte Zeit aufbewahrt. Daten in Backups werden nicht manuell gelöscht, sondern automatisch mit Ablauf des Backupzyklus überschrieben. Ein Zugriff auf gelöschte Daten aus Backups ist nicht vorgesehen.

18. Minderjährige

a. Nutzung nur durch Erwachsene

Die Plattform richtet sich ausschließlich an Unternehmen und volljährige Nutzer. Eine Nutzung durch Minderjährige ist nicht vorgesehen. Nutzer müssen bestätigen, dass sie mindestens 18 Jahre alt sind.

b. Ausschluss aktiver Erfassung

Es werden keine personenbezogenen Daten von Minderjährigen wissentlich erhoben oder verarbeitet. Sollte dennoch bekannt werden, dass solche Daten ohne Berechtigung erfasst wurden, werden sie umgehend gelöscht.

19. Änderungen der Datenschutzerklärung

a. Änderungsrechte

Hyptime behält sich vor, diese Datenschutzerklärung anzupassen, wenn technische, rechtliche oder betriebliche Entwicklungen dies erfordern. Die jeweils aktuelle Fassung ist jederzeit auf der Website abrufbar. Änderungen werden wirksam, sobald die neue Version veröffentlicht wurde, sofern sie nicht eine neue Einwilligung voraussetzen.

b. Benachrichtigung der Nutzer

Eine aktive Benachrichtigung erfolgt ausschließlich bei wesentlichen Änderungen, die die Rechte der Nutzer erheblich beeinflussen oder neue Einwilligungen erforderlich machen. In allen anderen Fällen genügt die Veröffentlichung der aktualisierten Datenschutzerklärung auf der Website.

20. Kontakt

a. Kontaktstelle für Datenschutz

Für Fragen zur Verarbeitung personenbezogener Daten, für Auskunftersuchen oder sonstige datenschutzrechtliche Anliegen kann der Verantwortliche unter den im Impressum genannten Kontaktdaten oder über die spezielle Datenschutzkontaktadresse erreicht werden:

Hyptime – Software Engineering
Erdal Cosgun
Hessische Straße 166
44339 Dortmund
Deutschland

Telefon: +49 231 8802 5269
E-Mail: info@hyptime.com

b. Beschwerden, Anliegen und Anfragen

Betroffene Personen können sich jederzeit mit Beschwerden, Anliegen oder Anfragen an Hyptime wenden. Anfragen werden gemäß den gesetzlichen Vorgaben der DSGVO bearbeitet.

Ausführung 2026-09