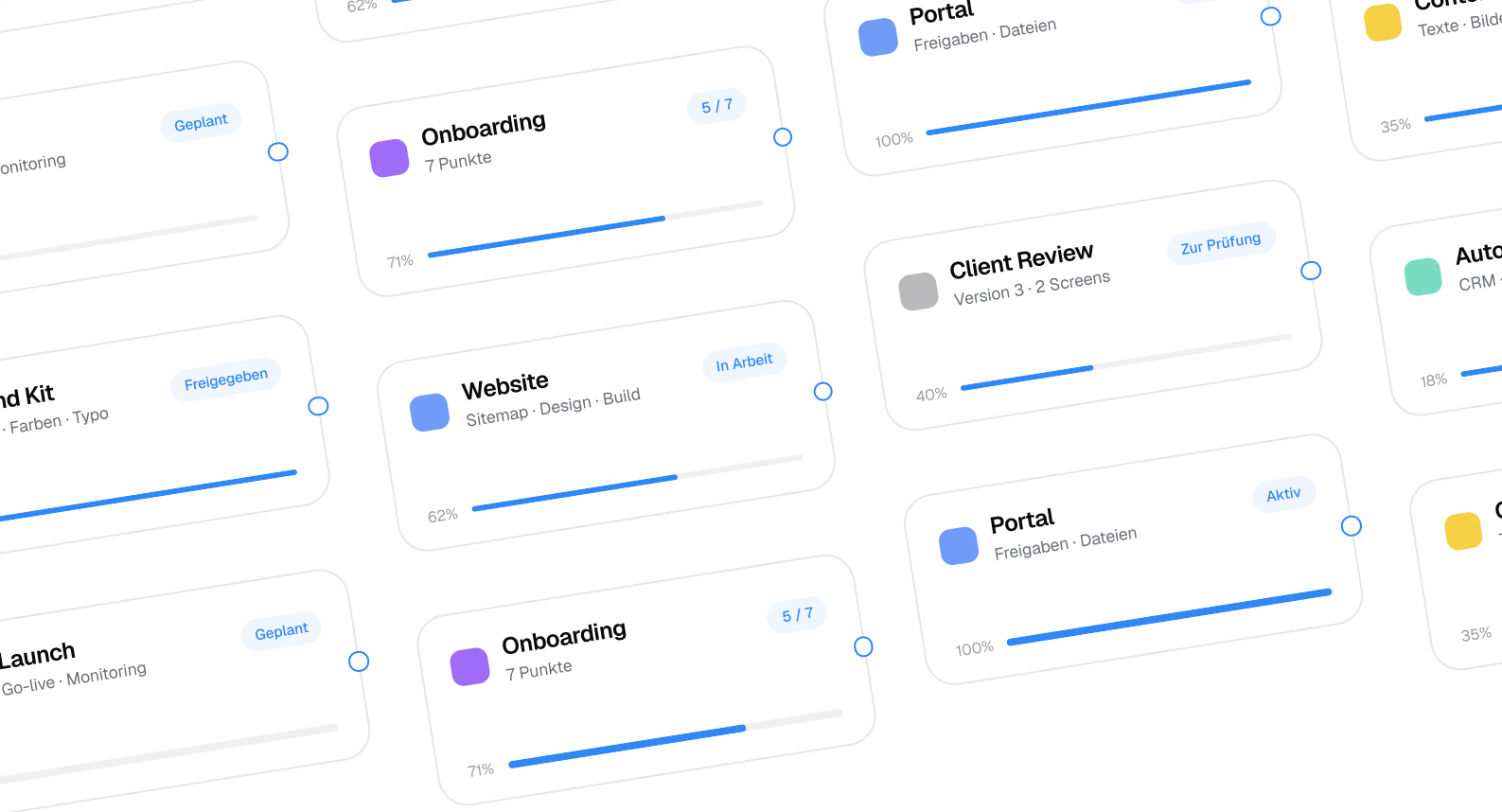




Technische und organisatorische Maßnahmen

Anlage zum Auftragsverarbeitungsvertrag

● v0.2 · Entwurf

Stand **Entwurf**

uvro

uvro

Marvin Habrichs · Rheinpromenade 4A, 40789 Monheim am Rhein · datenschutz@uvro.de · <https://uvro.de>

Technische und organisatorische Maßnahmen

Anlage zum Auftragsverarbeitungsvertrag

Dokument	Version	Stand	Status
toms	0.2	Entwurf	Entwurf

Dieses Dokument beschreibt die Maßnahmen nach Art. 32 DSGVO, mit denen UVRO personenbezogene Daten schützt. Aufgenommen sind nur Maßnahmen, die im UVRO-System umgesetzt sind; Maßnahmen des Hosting-Anbieters sind als solche gekennzeichnet.

01 Infrastruktur und physische Sicherheit

UVRO betreibt keine eigenen Server. Website, Kundenportal, Datenbank, Dateispeicher und Serverfunktionen laufen auf der Plattform Base44 und bei deren Infrastrukturdienstleistern (siehe Subprozessoren). Die physische Sicherheit der Rechenzentren liegt bei diesen Anbietern.

02 Zugang und Anmeldung

- Die Anmeldung am Kundenportal und an den internen Bereichen erfolgt über die Authentifizierung der Plattform Base44.
- Zugang zum Kundenportal erhalten nur Personen, die bei der Beauftragung angegeben oder vom Kunden bzw. von UVRO eingeladen wurden.
- Einmal-Links für das Onboarding sind zeitlich begrenzt (72 Stunden), in ihrer Anzahl beschränkt und werden nur als Hashwert (SHA-256) gespeichert.

03 Zugriffskontrolle und Trennung

- Rollenmodell mit getrennten Rechten für Administration, Projektteam und Kunden; innerhalb eines Kunden dürfen nur berechtigte Personen verbindlich beauftragen oder freigeben.
- Kunden sehen ausschließlich Daten ihres eigenen Unternehmens und Workspace. Die Trennung wird serverseitig über Zugriffsregeln der Datenbank (Row Level Security) und über Serverfunktionen durchgesetzt, die nur freigegebene Felder ausliefern.

-
- Zugangstoken verbundener Konten sind über die Anwendung für niemanden lesbar; nur Serverfunktionen können sie entschlüsseln.
-
- Test- und Live-Zahlungsumgebung sind strikt getrennt: getrennte Schlüssel, keine gegenseitige Ersatznutzung.
-

04

Übertragung und Verschlüsselung

-
- Übertragung ausschließlich verschlüsselt über HTTPS (TLS); uvro.de sendet HSTS.
-
- Zugangstoken verbundener Konten (Figma, GitHub, Google Drive) werden mit AES-256-GCM verschlüsselt gespeichert und kryptografisch an die jeweilige Verbindung gebunden.
-
- Dateien aus dem Brand-Onboarding werden in einem privaten Speicher abgelegt und nur über zeitlich begrenzte, signierte Links (300 Sekunden) ausgeliefert.
-
- Zahlungskarten- und Kontodaten werden ausschließlich von Stripe erhoben und erreichen die Systeme von UVRO nicht.
-

05

Datenminimierung und Pseudonymisierung

-
- Zur Begrenzung von Anfragen wird aus der IP-Adresse ein täglich wechselnder HMAC-Schlüssel gebildet; die IP-Adresse wird dafür nicht gespeichert.
-
- Im Nachweis einer Beauftragung wird die IP-Adresse gekürzt (IPv4 /24, IPv6 /48) und zusätzlich nur als HMAC gespeichert.
-
- Beim Import aus GitHub und Google Drive werden Dateien mit Zugangsdaten (etwa '.env', Schlüssel- und Zertifikatsdateien) ausgeschlossen und Textstellen, die wie Zugangsdaten aussehen, verworfen.
-
- Hochgeladene Onboarding-Dateien werden nach Dateiendung, Dateityp und Inhalt geprüft; unsichere SVG-Dateien werden abgelehnt.
-

06

Eingabekontrolle und Protokollierung

-
- Vertrags-, Freigabe- und Zahlungsereignisse werden in einem fortlaufend verketteten Ereignisprotokoll (Hashkette) mit handelnder Person und Zeitpunkt gespeichert. Kunden können Einträge weder anlegen noch ändern.
-
- Freigaben und Änderungswünsche im Kundenportal werden mit Version, Zeitpunkt und Person protokolliert.
-
- Jede Beauftragung wird mit den akzeptierten Dokumentversionen, deren Prüfsummen und einer Prüfsumme der Bestellung unveränderlich gespeichert.
-
- Versendete E-Mails werden mit Empfänger, Betreff, Vorlage und Status protokolliert.
-

Auftragskontrolle

- Unterauftragsverarbeiter werden nur eingesetzt, wenn ein Auftragsverarbeitungsvertrag mit geeigneten Garantien besteht; die Liste ist öffentlich unter [Subprozessoren](#) einsehbar.
- Webhooks des Zahlungsdienstleisters werden signaturgeprüft und idempotent verarbeitet.

Verfügbarkeit und Wiederherstellung

Datensicherung und Wiederherstellung der Datenbank und des Dateispeichers erfolgen durch den Hosting-Anbieter Base44.

Hinweis

Umfang, Häufigkeit und Aufbewahrung der Sicherungen bei Base44 sowie die Verschlüsselung ruhender Daten sind mit Base44 zu bestätigen.

Organisatorische Maßnahmen

- Zugriff auf Kundendaten erhalten nur die Personen, die am jeweiligen Projekt arbeiten.
- Personen, die für UVRO tätig werden, werden vor dem Zugriff auf Kundendaten zur Vertraulichkeit verpflichtet; beim Ausscheiden werden ihre Zugänge entzogen.
- Zugangsdaten und Schlüssel werden ausschließlich als Server-Secrets verwaltet und nicht im Quellcode gespeichert; ein automatischer Secret-Scan prüft jede Änderung.

Hinweis

Organisatorische Maßnahmen vom Inhaber zu bestätigen.

SHA-256 toms@0.2 · d3008859c5ffe6438be65b5590c6add680e704ff9f8c31057d89981255f35206