

DOKUMENTATION NACH ART. 32 DSGVO

Technische und organisatorische Maßnahmen

Sicherheit der Verarbeitung von Gesundheitsdaten (Art. 9 DSGVO)

DOKUMENT-NR.

BS-TOM-001

VERSION

3.1

STAND

28.08.2026

HERAUSGEBER

Pixel7 GmbH

Adressiert an

Gerichtlich zertifizierte Sachverständige, Pflegegutachterinnen und Pflegegutachter, ärztliche Gutachterinnen und Gutachter sowie deren Datenschutzbeauftragte und Auftraggeber.

Wozu dieses Dokument dient

Befundscanner verarbeitet Gesundheitsdaten — die sensibelste Kategorie personenbezogener Daten nach Art. 9 DSGVO. Wer als verantwortliche Stelle eine solche Verarbeitung an einen Dienstleister übergibt, muss sich davon überzeugen, dass dieser hinreichende Garantien bietet (Art. 28 Abs. 1 DSGVO). Dieses Dokument listet die dafür getroffenen technischen und organisatorischen Maßnahmen auf, mit denen Befundscanner diesen Anforderungen begegnet.

Grundlagen dieser Fassung

Interne TOM-Dokumentation Version 3 vom 22.07.2026, abgeglichen mit Anlage 3 des Auftragsverarbeitungsvertrags sowie der Datenschutz-Folgenabschätzung der heyData GmbH vom 30.06.2026 (durchgeführt nach ISO 29134).

Inhalt

- | | | | |
|----------|--|-----------|--|
| 1 | Rollen, Zweck und Geltungsbereich | 9 | Menschliche Kontrolle |
| 2 | Gegenstand der Verarbeitung | 10 | Organisatorische Maßnahmen |
| 3 | Weg eines Dokuments durch das System | 11 | Sub-Auftragsverarbeiter |
| 4 | Vertraulichkeit | 12 | OCR und Feldübernahme im Detail |
| 5 | Integrität | 13 | Rechtsgrundlagen, Normen und Standards |
| 6 | Verfügbarkeit und Belastbarkeit | 14 | Kontakt |
| 7 | Netzwerkisolation und Egress-Kontrolle | | |
| 8 | Datensparsamkeit und Löschung | | |

1 Rollen, Zweck und Geltungsbereich

Befundscanner ist eine Software-as-a-Service-Plattform der Pixel7 GmbH. Sie überträgt Inhalte medizinischer Befunddokumente (PDF) in vorbereitete Word-Vorlagen für Gutachten. Das System überträgt Inhalte wortgleich; es interpretiert nicht und trifft keine Entscheidungen.

Rolle	Stelle	Bedeutung
Verantwortlicher	Die Sachverständige bzw. der Sachverständige oder die Praxis, die Befundscanner nutzt	Bestimmt Zwecke und Mittel der Verarbeitung, erfüllt die Informationspflichten nach Art. 13/14 DSGVO gegenüber den Patientinnen und Patienten.
Auftragsverarbeiter	Pixel7 GmbH, Braillegasse 14, 1140 Wien, Österreich	Verarbeitet ausschließlich weisungsgebunden nach Art. 28 DSGVO. Dieses Dokument beschreibt die Maßnahmen nach Art. 32 DSGVO.
Datenschutzbeauftragter	heyData GmbH, Schützenstraße 5, 10117 Berlin	Benannter externer Datenschutzbeauftragter; hat die Datenschutz-Folgenabschätzung vom 30.06.2026 durchgeführt.
Betroffene	Patientinnen und Patienten	Indirekt betroffen — sie nutzen die Plattform nicht selbst und stehen in keinem direkten Kontakt zum System.

Tabelle 1: Datenschutzrechtliche Rollen.

Geltungsbereich. Die beschriebenen Maßnahmen gelten für den gesamten produktiven Betrieb von Befundscanner unter app.befundscanner.at, einschließlich der vorgelagerten Texterkennung, der Feldübernahme, der Speicherung, der Prüfoberfläche und des Dokumentexports. Sie gelten nicht für Systeme der verantwortlichen Stelle selbst — etwa deren lokale Arbeitsplätze, E-Mail-Postfächer oder Ablagen, in denen ein exportiertes Gutachten anschließend weiterverarbeitet wird.

2 Gegenstand der Verarbeitung

Den Kern der Verarbeitung bilden vollständige medizinische Befunddokumente. Sie enthalten regelmäßig Diagnosen, Anamnesen, Befundtexte sowie Labor- und Bildgebungsergebnisse und sind damit besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO.

Datenkategorie	Inhalt	Einstufung
Befunddokumente	Hochgeladene PDF im Vollinhalt	Art. 9 DSGVO
Übernommene Feldwerte	Art des Dokuments, Dokumentdatum, ausstellende Ärztin bzw. Einrichtung, Diagnosen, Fachrichtung, Befundtext, Anamnese, Therapien und weitere von der Praxis definierte Felder	Art. 9 DSGVO
Positionsdaten	Bounding-Box-Koordinaten (x/y/w/h, normalisiert) zur Markierung der Fundstelle im Dokument — ohne Textinhalt	kein direkter Personenbezug
Praxis-Stammdaten	Praxisname, Adresse, Telefonnummer; Titel, Vor- und Nachname, E-Mail-Adresse und Telefonnummer der Nutzenden	Art. 6 DSGVO
Zugangsdaten	E-Mail-Adresse und Passkey-Credential-ID (bei Hanko)	Art. 6 DSGVO
Abrechnungsdaten	Zahlungsmittel-Token und Abonnement-Status (bei Stripe) — der vollständige Zahlungsmitteldatensatz liegt Pixel7 nie vor	Art. 6 DSGVO
Protokolldaten	Aktion, Ressourcentyp und -kennung, Zeitstempel; ausdrücklich keine medizinischen Inhaltswerte	Art. 6 DSGVO

Tabelle 2: Verarbeitete Datenkategorien.

3 Weg eines Dokuments durch das System

Die folgende Übersicht zeigt für jeden Schritt, wo Daten liegen und in welchem Zustand. Sie ist die Grundlage für das Verständnis der Abschnitte 4 bis 8.

Schritt	Vorgang	Ort und Zustand der Daten
1	Upload	Das PDF wird über TLS 1.3 an die Anwendung übertragen und in den Objektspeicher gelegt. Beim Upload wird ein SHA-256-Hash gebildet.
2	Seitenzerlegung	Das Dokument wird seitenweise zerlegt. Jede Seite wird vor dem Ablegen verschlüsselt. Danach wird das Original-PDF unverzüglich aus dem Objektspeicher gelöscht.
3	Texterkennung	Die Seite wird an den selbst betriebenen OCR-Dienst in den Niederlanden übergeben. Der erkannte Text existiert ausschließlich im Arbeitsspeicher des Verarbeitungs-Workers.
4	Feldübernahme	Ein selbst betriebenes Sprachmodell übernimmt die Werte der definierten Felder aus dem erkannten Text. Anfrage und Antwort bleiben im Arbeitsspeicher und werden nicht protokolliert.
5	Speicherung	Die übernommenen Feldwerte werden verschlüsselt in der Datenbank abgelegt. Der erkannte Text selbst wird nicht gespeichert.
6	Prüfung	Die Sachverständige prüft jeden Wert in einer geteilten Ansicht neben dem Originaldokument und akzeptiert, korrigiert oder blendet ihn aus.
7	Export	Das Dokument wird auf Abruf erzeugt und direkt an den Browser gestreamt. Es wird nicht serverseitig gespeichert.
8	Löschung	Spätestens 24 Stunden nach Anlage des Falls werden alle Falldaten kaskadierend und unwiderruflich gelöscht — früher, wenn die Nutzerin die Löschung selbst auslöst.

Tabelle 3: Verarbeitungsschritte und Datenzustand.

4 Vertraulichkeit

4.1 Zugangskontrolle

- **Passkeys als Regelverfahren.** Die Anmeldung erfolgt phishing-resistent über Passkeys nach WebAuthn/FIDO2 (Hanko GmbH, Serverstandort Deutschland) mit zwingender Mehr-Faktor-Authentifizierung.
- **Gehärteter Fallback.** Der alternative Anmeldeweg über E-Mail und Passwort unterliegt Vorgaben zur Passwortstärke und einer Begrenzung auf höchstens fünf Anfragen pro Minute und IP-Adresse.
- **Automatische Abmeldung.** Nach 30 Minuten ohne Aktivität wird die Sitzung beendet; eine erneute Anmeldung ist erforderlich.
- **Serverseitige Prüfung jeder Anfrage.** Eine Middleware prüft das Sitzungstoken auf Signatur, Ablaufzeit und Inhalt und weist ungültige Token ab.
- **Physische Sicherheit.** Betrieb in nach ISO/IEC 27001 zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland. Physischer Zugang ausschließlich für autorisiertes Personal des Rechenzentrumsbetreibers.

4.2 Rollen- und Rechtekonzept

- Dreistufiges Rollenmodell: Inhaberin bzw. Inhaber (volle Rechte), Administration (Verwaltung ohne Abrechnungsbefugnis), Teammitglied (eingeschränkter Zugriff).
- Need-to-Know: Zugriff nur auf das für die jeweilige Aufgabe Erforderliche.
- Die Praxiskennung wird stets aus der verifizierten Sitzung abgeleitet und niemals aus Eingaben der Anfrage übernommen. Manipulierte Adressparameter können daher keinen fremden Datenbestand adressieren.

4.3 Verschlüsselung während der Übertragung

Sämtliche Übertragungen zwischen Browser, Anwendung, Verarbeitungs-Worker, Objektspeicher und den Diensten für Texterkennung und Feldübernahme laufen über TLS 1.3.

4.4 Verschlüsselung ruhender Daten

Ruhende Patientendaten werden mit XChaCha20-Poly1305 aus der auditierten Bibliothek libsodium verschlüsselt. Die Schlüsselhierarchie folgt NIST SP 800-57 und NIST SP 800-111:

Praxis-Schlüssel (DEK)	je Praxis ein eigener Datenschlüssel
↓ gesichert durch	
Hauptschlüssel (KEK)	als geschütztes Betriebsgeheimnis getrennt von den Daten auf dedizierter EU-Infrastruktur gehalten
Zusatzdaten (AAD)	die Praxiskennung geht als authentifizierte Zusatz-information in jede Ver- und Entschlüsselung ein

- Feldwerte und Korrekturprotokolle liegen ausschließlich in verschlüsselten Spalten; Klartext wird nicht gespeichert.
- Auch die Seitenbilder im Objektspeicher werden vor dem Ablegen verschlüsselt. Zugriff darauf erfolgt nur über kurzlebige, signierte Abruf-Adressen.
- Schlüsselmaterial wird nach Gebrauch im Arbeitsspeicher überschrieben.
- Auch die Datenbank-Sicherungskopien sind verschlüsselt (Aufbewahrung siehe Abschnitt 6).

4.5 Mandantentrennung

Die Trennung der Praxen ist doppelt abgesichert — einmal auf Ebene der Datenbank, einmal kryptografisch:

Ebene	Maßnahme	Wirkung
Datenbank	Row Level Security auf allen mandantenbezogenen Tabellen, zusätzlich als FORCE gesetzt — die Regel gilt auch für die Eigentümerrolle der Tabelle.	Ohne gesetzten Mandantenkontext liefert jede Abfrage null Zeilen (fail-closed). Ein vergessener Filter im Anwendungscode führt nicht zu fremden Daten, sondern zu keinen Daten.
Kryptografie	Die Praxiskennung dient als authentifizierte Zusatzinformation der Verschlüsselung.	Selbst wenn ein Datensatz einer fremden Praxis erreichbar wäre, schläge die Entschlüsselung fehl. Die Trennung ist damit nicht nur eine Zugriffsregel, sondern rechnerisch verankert.

Tabelle 4: Zwei unabhängige Schichten der Mandantentrennung.

5 Integrität

- **Eingabevalidierung.** Jede Schnittstelle prüft eingehende Daten gegen ein festes Schema; unbekannte Felder werden abgewiesen.
- **Prüfsumme beim Upload.** Für jedes hochgeladene Dokument wird ein SHA-256-Hash gebildet.
- **Revisionssicheres Protokoll.** Das Protokoll aller sicherheitsrelevanten Aktionen ist ausschließlich fortschreibend. Änderungen und Löschungen einzelner Einträge sind auf Datenbankebene per Regel untersagt, nicht nur im Anwendungscode.
- **Protokoll-Bereinigung.** Ein zentraler Filter entfernt medizinische Inhaltswerte aus allen Protokollen. Erlaubt sind ausschließlich Kennungen, Aktionstypen, Zeitstempel und Zähler. Fehlermeldungen enthalten nur Fehlerklasse und Status, nie den Inhalt eines Dokuments.
- **Fehlertoleranz ohne Datenverlust.** Übersteigt ein Dokument die Verarbeitungsgrenze des Sprachmodells, wird die Verarbeitung mit einem klaren Fehler abgebrochen, statt den Text still zu kürzen.

6 Verfügbarkeit und Belastbarkeit

- **Hosting.** Anwendung, Datenbank und Verarbeitungs-Worker laufen auf dedizierter Infrastruktur der Hetzner Online GmbH in Falkenstein und Nürnberg. Die Rechenzentren des Infrastrukturdienstleisters sind nach ISO/IEC 27001 zertifiziert; für die Plattform selbst besteht keine eigene Zertifizierung.
- **Sicherungskopien.** Verschlüsselte, serverseitige Datenbank-Snapshots ausschließlich zur Ausfallsicherheit (Art. 32 DSGVO). Aufbewahrung höchstens **7 Tage**, danach rollierend überschrieben.
- **Verarbeitungswarteschlange.** Aufträge werden mit gestuftem Wiederholungs- und Wartezeitverfahren abgearbeitet. Ein Wächterprozess erkennt hängende Aufträge und setzt sie zurück.
- **Gehärtete Systemarchitektur** auf verwalteter, zertifizierter Infrastruktur mit systematischen Sicherheitsaktualisierungen.

Begrenzung der Anfragelast

Bereich	Grenze	Bezug
Schnittstellen allgemein	100 Anfragen/Minute	je Nutzerin bzw. Nutzer
Anmeldung	5 Anfragen/Minute	je IP-Adresse
Upload	10 Anfragen/Minute	je Nutzerin bzw. Nutzer
Abrechnung	20 Anfragen/Minute	je Nutzerin bzw. Nutzer

Tabelle 5: Begrenzung der Anfragelast (Schutz vor Überlastung und automatisierten Angriffen).

7 Netzwerkisolation und Egress-Kontrolle

Der empfindlichste Punkt einer KI-gestützten Verarbeitung ist die Frage, wohin Daten das eigene System verlassen. Diese Frage ist hier nicht organisatorisch, sondern technisch beantwortet — an drei voneinander unabhängigen Stellen.

Sperre	Wirkungsweise
Netzwerk-Firewall	Die Dienste für Texterkennung und Feldübernahme sind über eine Firewall mit Adressfreigabe abgesichert und ausschließlich von der festen IP-Adresse des Verarbeitungs-Workers erreichbar. Über das öffentliche Internet sind sie nicht ansprechbar.
Compliance-Gate im Code	Vor jeder ausgehenden Verbindung prüft eine im Quellcode verankerte Sperre, ob der Betrieb auf selbst betriebener EU-Infrastruktur ausdrücklich bestätigt ist. Fehlt die Bestätigung, bricht die Verarbeitung mit einem harten Fehler ab, bevor ein einziges Byte das System verlässt (fail-closed). Ein unbekannter Anbieterwert führt zum Abbruch, nicht zu einer stillen Ausweichverarbeitung.
Bausperre im Frontend	Eine Regel im Werkzeugkasten der Entwicklung verhindert, dass Module für Texterkennung oder Feldübernahme in die Auslieferungsschicht importiert werden. Der ausgehende Datenverkehr bleibt damit strukturell auf den Verarbeitungs-Worker beschränkt.

Tabelle 6: Drei unabhängige Sperren gegen unbeabsichtigten Datenabfluss.

8 Datensparsamkeit und Löschung

Das wirksamste Mittel gegen den Missbrauch sensibler Daten ist, sie gar nicht erst aufzubewahren. Befundscanner speichert deshalb so wenig und so kurz wie technisch möglich.

Datenkategorie	Frist	Mechanismus
Erkannter Text und Modell-Anfragen	keine Speicherung	Nur im Arbeitsspeicher des Workers; nach der Übernahme verworfen. Auch keine Ablage in Fehlerprotokollen.
Original-PDF	unverzüglich	Löschung aus dem Objektspeicher direkt nach der seitenweisen, verschlüsselten Ablage.
Verschlüsselte Seitenbilder	max. 24 Stunden	Teil der kaskadierenden Fall-Löschung.
Verschlüsselte Feldwerte und Korrekturprotokoll	max. 24 Stunden	Teil der kaskadierenden Fall-Löschung.
Patientenfall insgesamt	max. 24 Stunden	Ab Anlage des Falls; ein Countdown in der Oberfläche zeigt die verbleibende Zeit an.
Gutachten-Export	keine Speicherung	Wird auf Abruf erzeugt und direkt an den Browser gestreamt.
Protokoll sicherheitsrelevanter Aktionen	dauerhaft	Enthält ausschließlich Kennungen, Aktionstypen und Zeitstempel, keine medizinischen Inhaltswerte.
Sicherungskopien der Datenbank	max. 7 Tage	Verschlüsselt, ausschließlich zur Ausfallsicherheit; rollierend überschrieben.
Praxis-Stammdaten	Vertragsdauer	Löschung nach Beendigung der Geschäftsbeziehung.
Abrechnungsdaten bei Stripe	7 Jahre	Gesetzliche steuerrechtliche Aufbewahrungspflicht.

Tabelle 7: Löschrufen je Datenkategorie.

Wie die 24-Stunden-Löschung abgesichert ist

Die Löschung hängt nicht an einem einzelnen Auslöser. Drei Wege führen durch **dieselbe** Löschroutine: der zeitgesteuerte Systemlauf, eine unabhängige Schleife im Verarbeitungs-Worker und der manuelle Löschbefehl in der Oberfläche. Fällt ein Weg aus, greifen die anderen. Ein Mehrfachlauf ist unschädlich: Nur der Durchlauf, der den Datensatz tatsächlich entfernt, löst die Löschung im Objektspeicher und den Protokolleintrag aus. Die Reihenfolge ist dabei festgelegt — erst wird die Datenbanktransaktion bestätigt, dann werden die Dateien gelöscht. So können bei einem Abbruch keine verwaisten Dateien zurückbleiben.

9 Menschliche Kontrolle

Befundscanner ist ein Assistenzsystem. Es trifft keine automatisierten Entscheidungen mit rechtlicher Wirkung im Sinne von Art. 22 DSGVO.

- Kein übernommener Wert gelangt automatisch in das fertige Dokument. Jeder Wert wird in einer geteilten Ansicht neben dem Originaldokument vorgelegt und muss geprüft, korrigiert oder ausdrücklich übernommen werden.
- Ein Feld, das in der Prüfung erschienen ist, wird niemals selbsttätig entfernt. Der einzige Weg, es aus dem Dokument zu nehmen, ist die ausdrückliche Ausblenden-Schaltfläche.
- Die fachliche Verantwortung für den Inhalt des Gutachtens liegt unverändert und vollständig bei der bestellten Sachverständigen bzw. dem bestellten Sachverständigen.
- Die Prüfseite ist mit einer technischen Drucksperrung versehen.
- Datenschutz-Hinweise, ein Informationsfenster und der sichtbare 24-Stunden-Countdown sind fest in die Oberfläche eingebaut.

10 Organisatorische Maßnahmen

- **Vertraulichkeitsverpflichtung** aller Mitarbeitenden nach Art. 28 Abs. 3 lit. b DSGVO.
- **Need-to-Know beim Produktionszugang.** Der Zugang zur Produktivumgebung ist auf den zwingend erforderlichen Personenkreis begrenzt.
- **Austritt von Schlüsselpersonen.** Sofortige Deaktivierung aller Zugänge und verpflichtende Rotation des Hauptschlüssels mit Neuverschlüsselung der Praxis-Schlüssel.
- **Belehrung zu Art. 9 DSGVO.** Alle Personen mit Produktionszugang sind ausdrücklich über ihre Pflichten im Umgang mit Gesundheitsdaten belehrt.
- **Externer Datenschutzbeauftragter:** heyData GmbH. Neue Verarbeitungswege für Gesundheitsdaten werden vor Inbetriebnahme dort vorgelegt.
- **Click-Through-AVV.** Jede Praxis stimmt der Auftragsverarbeitungsvereinbarung vor der ersten eigenen Verarbeitung aktiv zu. Die Zustimmung wird revisionssicher und fortschreibend dokumentiert; bei einer neuen Vertragsversion wird erneut zugestimmt.
- **Jährliche Neubewertung** der Verarbeitungszwecke im Rahmen eines Datenschutzaudits.

11 Sub-Auftragsverarbeiter

Mit allen genannten Dienstleistern bestehen Auftragsverarbeitungsverträge nach Art. 28 DSGVO. Sämtliche Verarbeitung von Gesundheitsdaten findet auf Infrastruktur innerhalb der Europäischen Union statt; eine Übermittlung in Drittländer findet nicht statt. Standardvertragsklauseln sind für diesen Verarbeitungsweg daher nicht erforderlich.

Anbieter	Zweck	Standort	Art.-9-Daten
Hetzner Online GmbH	PostgreSQL-Datenbank, S3-kompatibler Objektspeicher, dedizierte Server für Anwendung und Verarbeitungs-Worker; verschlüsselte Sicherungskopien (max. 7 Tage)	Falkenstein / Nürnberg, Deutschland	ja — verschlüsselt
Media Trooper GmbH	Texterkennung (selbst betriebenes PaddleOCR-VL) und Feldübernahme (selbst betriebenes Qwen3-30B über vLLM); ohne Datenaufbewahrung, ohne Anfrageprotokollierung, ohne Modelltraining	Niederlande (EU)	ja — nur flüchtig im Arbeitsspeicher
Hanko GmbH	Authentifizierung (Passkeys/FIDO2, MFA, Sitzungsverwaltung)	Heidelberg, Deutschland	nein
IONOS SE	Transaktionaler E-Mail-Versand für Systembenachrichtigungen	Deutschland	nein
Stripe Payments Europe, Ltd.	Zahlungsabwicklung und Abrechnung	Irland (EU)	nein

Tabelle 8: Sub-Auftragsverarbeiter (Anlage 4 des AVV).

12 OCR und Feldübernahme im Detail

Weil dieser Verarbeitungsschritt bei Sachverständigen erfahrungsgemäß die meisten Rückfragen auslöst, ist er hier gesondert aufgeschlüsselt.

- Texterkennung und Feldübernahme laufen auf **dedizierten, exklusiv für Befundscanner reservierten Servern in der EU**, betrieben durch die Media Trooper GmbH in den Niederlanden. Externe Cloud-KI-Dienste kommen nicht zum Einsatz; es werden keine Daten an externe

KI-Anbieter übermittelt.

- Auf diesen Servern findet **keine Datenaufbewahrung** und **keine Protokollierung der Anfragen** statt. Die Verarbeitung erfolgt ausschließlich im Arbeitsspeicher für die Dauer der Berechnung.
- **Kein Modelltraining** mit Patientendaten — weder durch Pixel7 noch durch den Dienstleister. Dies ist vertraglich festgeschrieben.
- Die Modelle sind auf Wortgleichheit ausgelegt: Sie übernehmen den Wortlaut aus dem Dokument, statt ihn umzuformulieren. Wie wörtlich das im Betrieb tatsächlich gelingt, wird laufend gemessen und ist in einer eigenen Methodendokumentation offengelegt.

13 Rechtsgrundlagen, Normen und Standards

Rechtsgrundlagen der Verarbeitung

Datenkategorie	Rechtsgrundlage
Gesundheitsdaten der Patientinnen und Patienten	Art. 6 Abs. 1 lit. c bzw. lit. e DSGVO in Verbindung mit Art. 9 Abs. 2 lit. g DSGVO (erhebliches öffentliches Interesse), ergänzend Art. 9 Abs. 2 lit. f DSGVO (Rechtsansprüche im Rahmen von Gerichtsverfahren) — getragen durch den hoheitlichen bzw. gesetzlichen Auftrag an die Sachverständigen.
Praxis-, Zugangs- und Abrechnungsdaten	Art. 6 Abs. 1 lit. b DSGVO (Erfüllung des Nutzungsvertrags).
Protokolldaten	Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an Informations- und Systemsicherheit).

Tabelle 9: Rechtsgrundlagen nach Einstufung durch die Datenschutz-Folgenabschätzung. Die abschließende Festlegung obliegt der verantwortlichen Stelle.

Herangezogene Normen und Standards

- DSGVO (EU) 2016/679 — insbesondere Art. 5, 9, 25, 28, 32 und 35
- ISO 29134 — Methodik der durchgeführten Datenschutz-Folgenabschätzung
- Grundprinzipien der ISO/IEC 27001
- NIST SP 800-57 und NIST SP 800-111 — Schlüsselverwaltung und Speicherverschlüsselung
- OWASP Top 10 (2021) — Grundlage der internen Sicherheitscheckliste
- FIDO2 / WebAuthn — Authentifizierung

14 Kontakt

Auftragsverarbeiter	Pixel7 GmbH, Braillegasse 14, 1140 Wien, Österreich
Produkt	Befundscanner · app.befundscanner.at
Ansprechpartner	Piere Paukovitsch · piere@pixel7.at
Datenschutzbeauftragter	heyData GmbH, Schützenstraße 5, 10117 Berlin · support@heydata.eu
Weitere Dokumente	Auftragsverarbeitungsvertrag und Datenschutz-Folgenabschätzung stehen auf Anfrage sowie im Konto unter „Datenschutz“ zum Abruf bereit.
Dokument	BS-TOM-001 · Version 3.1 · Stand 28.08.2026

Dieses Dokument beschreibt technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Es ist keine Rechtsberatung, ersetzt keine eigene Prüfung durch die verantwortliche Stelle und begründet keine über den Auftragsverarbeitungsvertrag hinausgehenden Zusicherungen.