NextGen Consulting
HR & AI CONSULTING

VERGÜTUNGSANALYSE · DATENSCHUTZKONZEPT · JUNI 2026

Datenschutz, der Vertrauen schafft.

Wie die Vergütungsanalyse die Gehalts- und Personaldaten Ihrer Mitarbeitenden schützt — technisch nachweisbar und rechtlich sauber.

VERGÜTUNGSANALYSE
FÜR GESCHÄFTSFÜHRUNG, HR & DATENSCHUTZBEAUFTRAGTE

JUNI 2026
SASCHA KUBAK · SASCHA.KUBAK@NEXT-GEN-CONSULTING.DE

Datenschutz auf zwei Ebenen erklärt.

Diese Präsentation spricht Geschäftsführung & HR **und** Datenschutzbeauftragte an. Die Kernbotschaft steht jeweils in der Überschrift, die prüffähige Detailtiefe in den blauen Hinweisboxen darunter.

01 **So schützen wir die Daten**
Pseudonymisierung im Browser · Datenminimierung · Privacy by Design
~ 5 min
SLIDES 3–6

02 **Ehrlich & rechtssicher**
Pseudonym ≠ anonym · Rollen & AVV · Rechtsgrundlage · EU-Hosting
~ 7 min
SLIDES 7–11

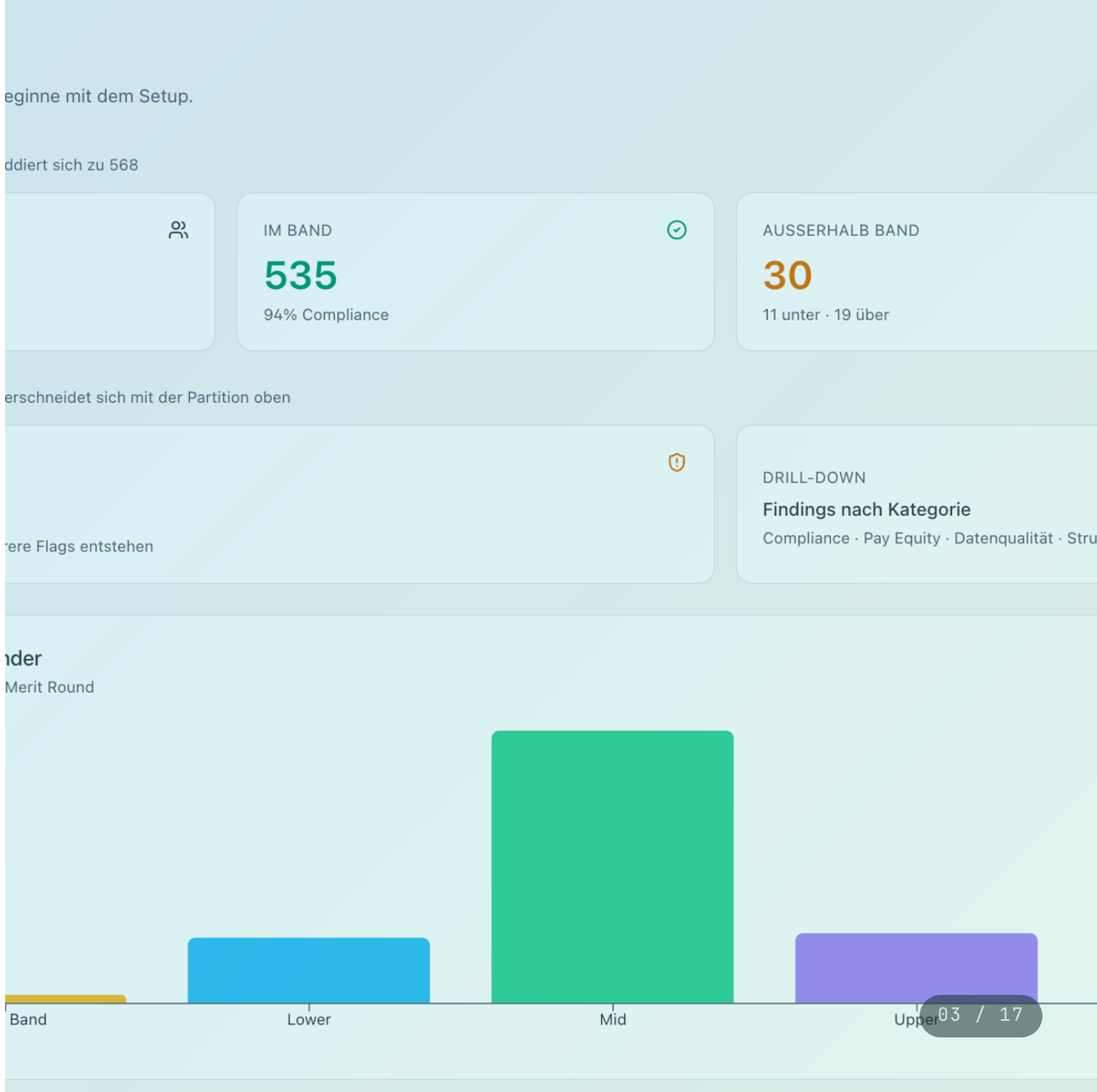
03 **Betriebsmodelle: SaaS vs. On-Premise**
Zwei Hosting-Optionen · Datenschutz-Vergleich · Empfehlung On-Premise
~ 5 min
SLIDES 12–14

04 **Rechte, Pflichten & Fazit**
Betroffenenrechte · Löschkonzept · DSFA & Betriebsrat · nächste Schritte
~ 4 min
SLIDES 15–17

TEIL 01 · SCHUTZKONZEPT

So schützen wir die Daten.

Datenschutz ist in der Vergütungsanalyse keine nachträgliche Schicht — er ist in die Architektur eingebaut. Drei Prinzipien tragen das.



Klarnamen verlassen Ihren Browser nicht.

Die Pseudonymisierung passiert bereits auf dem Rechner Ihrer HR — bevor irgendein Datum unsere Server erreicht.

SCHRITT 1

Excel im Browser

Ihre Gehaltsliste wird lokal im Browser eingelesen — nicht hochgeladen.

SCHRITT 2

Pseudonym statt Name

Die Personalnummer wird mit einem geheimen Schlüssel zu einem nicht umkehrbaren Code (SHA-256) verrechnet.

SCHRITT 3

Nur Codes an uns

An unsere Server geht ausschließlich pseudonymisiertes Datenmaterial — keine Namen.

Für die DS-Prüfung: Client-seitiges SHA-256(Salt + Pers.-Nr.). Die API erzwingt ein Strict-Schema, das jedes Klarnamen-Feld (name, email, manager) aktiv abweist. Roh-Excel wird zu keinem Zeitpunkt serverseitig gespeichert.

Nur, was die Analyse wirklich braucht.

Verarbeitet — pseudonymisiert

- Pseudonym statt Klarname
- Geschlecht (für die Pay-Gap-Analyse)
- Geburts- und Eintrittsjahr
- Gehalt, Bonus, Wochenstunden
- Position, Level, Abteilung, Standort
- Manager-Pseudonym (für Favoritismus-Check)

Bewusst NICHT gespeichert

- Klarnamen der Mitarbeitenden
- Klartext-Personalnummern
- Adressen oder Kontaktdaten
- Klartext-IP-Adressen (nur gehasht)
- Freitext-Personalakten / Bewertungen

Zweckbindung: Das Geschlecht wird ausschließlich für die geschlechtsbezogene Entgeltanalyse verwendet — nicht für andere Auswertungen.

Schutz ist eingebaut, nicht aufgesetzt.

Technische Maßnahmen

- Pseudonymisierung im Browser
- Strict-Schema weist Klarnamen ab
- Eigener Schlüssel je Kunde — keine Verkettung
- Verschlüsselung & rollenbasierter Zugriff

Nachvollziehbarkeit

- Lückenloses Audit-Log (mit gehashter IP)
- Unveränderbare Stichtags-Snapshots
- Signierte PDF-Reports (SHA-256-Prüfsumme)
- Trennung Admin- / Kundenrolle

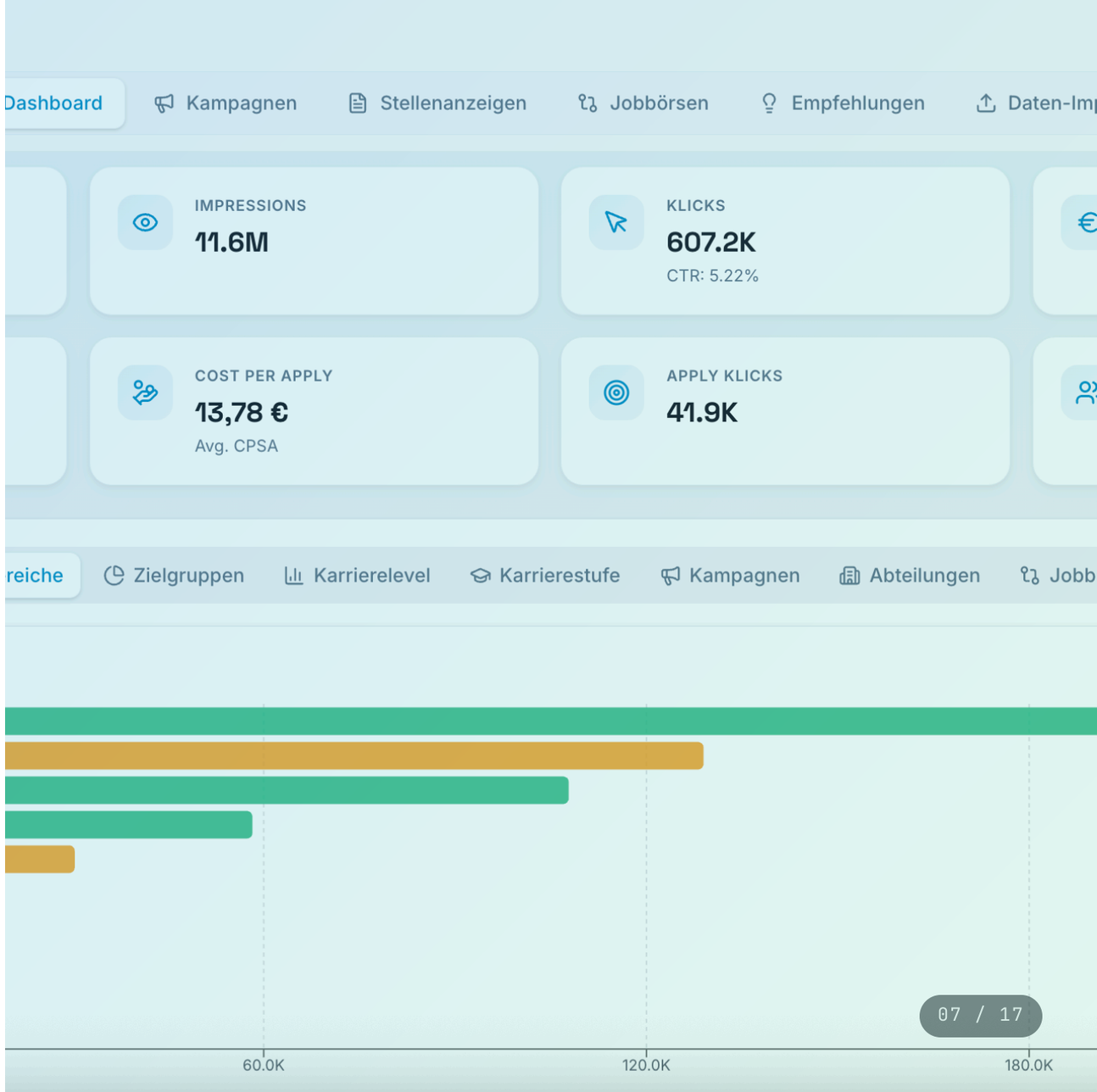
Für die DS-Prüfung: Diese technischen und organisatorischen Maßnahmen (TOMs nach Art. 32 DSGVO) sind dokumentiert und im Auftragsverarbeitungsvertrag referenzierbar.

TEIL 02 · TRANSPARENZ & RECHT

Ehrlich bleiben. Rechtssicher arbeiten.

Wir versprechen keine Anonymität, die wir nicht halten können. Stattdessen benennen wir die Grenzen offen — und sichern sie technisch und vertraglich ab.

Vergütungsanalyse · Datenschutz



Pseudonym ist nicht anonym — und das sagen wir.

Pseudonymisierte Daten bleiben rechtlich personenbezogen (Erwägungsgrund 26 DSGVO). Wir managen dieses Restrisiko aktiv, statt es zu verschweigen.

RISIKO

Re-Identifikation

Wer Schlüssel und Originalliste besitzt, kann rückverknüpfen. In kleinen Gruppen genügt schon die Kombination aus Position, Standort und Geschlecht.

UNSERE ANTWORT

Aktiv begrenzt

Schlüssel-Zugriff nur für Import-Berechtigte · Auswertungen erst ab Mindestgruppengröße · Einzelfälle nur für berechtigte Rollen und protokolliert.

Für die DS-Prüfung: Mindestgruppengröße $k \geq 5$ (k-Anonymität). Unterschreitet eine Gruppe diese Schwelle, wird die Kennzahl unterdrückt oder aggregiert ausgewiesen.

Klare Rollen, klarer Vertrag.

SIE

Verantwortlicher

Sie bestimmen Zweck und Mittel — es sind die Daten Ihrer Beschäftigten.

NEXTGEN CONSULTING

Auftragsverarbeiter

Wir verarbeiten ausschließlich weisungsgebunden in Ihrem Auftrag.

CLOUDFLARE

Unterauftrag

Hosting in der EU — als Unterauftragsverarbeiter gelistet.

Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Ist **verpflichtend** — und wir stellen ihn bereit, inklusive vollständiger Unterauftragsverarbeiter-Liste und der dokumentierten Schutzmaßnahmen.

Es gibt einen klaren Rechtsrahmen.

EU-RECHT

Entgelttransparenzrichtlinie 2023/970

Pflicht zum Gender-Pay-Gap-Reporting — Umsetzung bis Juni 2026. (Art. 6 (1) c DSGVO)

BESCHÄFTIGUNG

§ 26 BDSG

Verarbeitung von Beschäftigtendaten für Zwecke des Arbeitsverhältnisses.

ABWÄGUNG

Berechtigtes Interesse

Diskriminierungsfreie, konsistente Vergütungsstruktur. (Art. 6 (1) f DSGVO)

Aus der Pflicht wird ein Vorteil

Die EU-Richtlinie macht die Analyse nicht nur zulässig — sie macht sie ab 2026 zur **gesetzlichen Pflicht**. Wer jetzt sauber aufsetzt, ist vorbereitet.

Ihre Daten bleiben in der EU.

STANDORT

EU-Datenresidenz aktiv

Betrieb auf Cloudflare (Anwendung, Datenbank, Datei-Speicher). Die Daten ruhen in europäischen Rechenzentren.

EHRLICH BENANNT

Restrisiko abgesichert

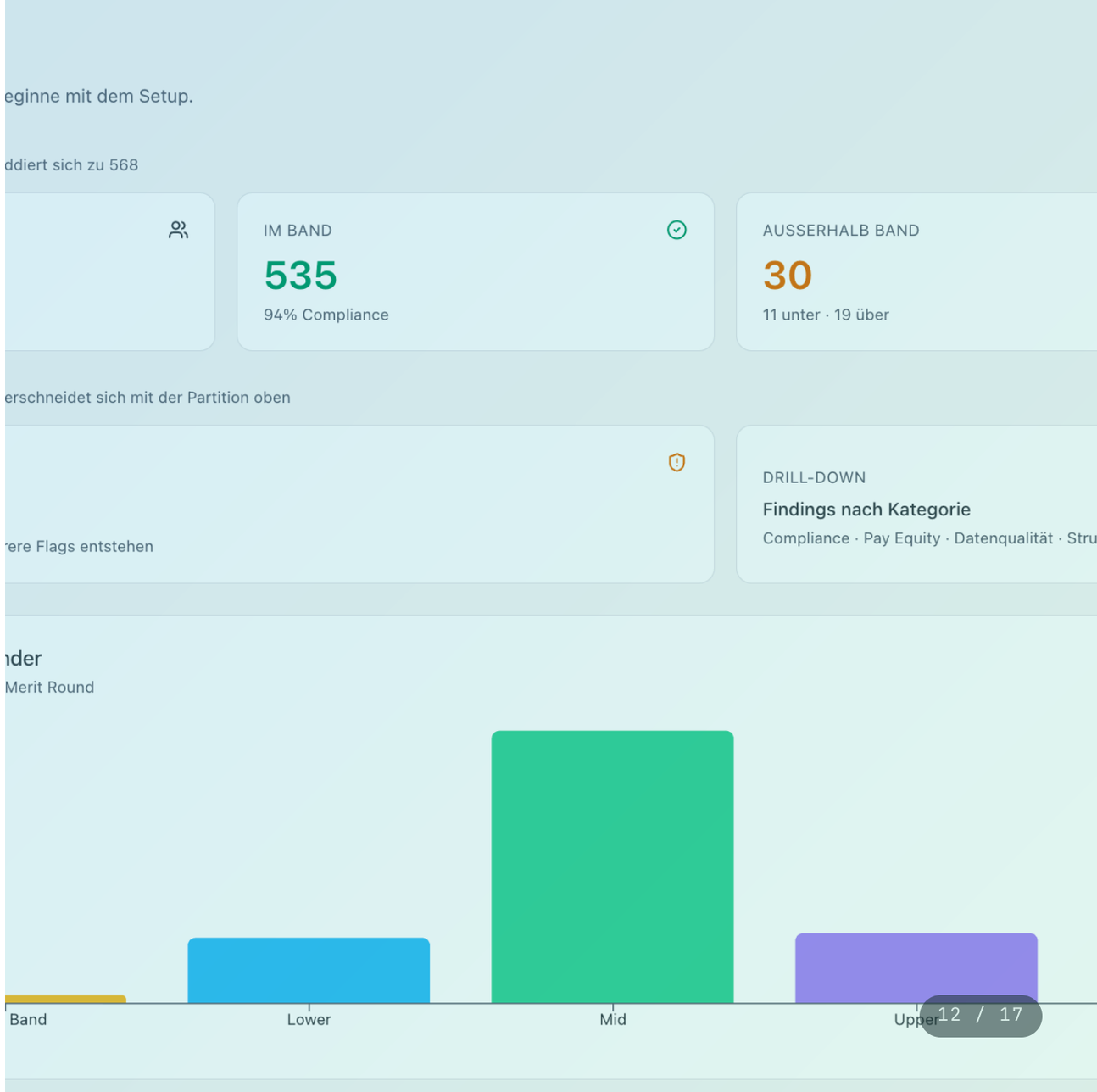
Cloudflare ist ein US-Konzern (CLOUD Act). Die EU-Residenz reduziert das Risiko; vollständig abgesichert über Standardvertragsklauseln im AVV.

Für die DS-Prüfung: Drittlandtransfer nach Art. 44 ff. DSGVO über Standardvertragsklauseln (SCCs) und ein Transfer-Impact-Assessment im AVV abgesichert.

TEIL 03 · BETRIEB & HOSTING

Zwei Betriebs-modelle. Eine klare Empfehlung.

Die Vergütungsanalyse lässt sich als Cloud-Dienst (SaaS) durch uns betreiben — oder bei Ihnen im Haus (On-Premise). Datenschutzrechtlich macht das den größten Unterschied.



SaaS oder On-Premise?

OPTION A · SAAS / CLOUD

Wir betreiben es

- NGC = Auftragsverarbeiter → AVV zwingend
- Daten liegen bei uns (Cloudflare, EU-Residenz)
- Drittland-Thema → SCCs + TIA nötig
- Wir verantworten Betrieb, Updates, Backups
- Vorteil: null Betriebsaufwand für Sie

OPTION B · ON-PREMISE — EMPFOHLEN

Sie hosten es im Haus

- Daten verlassen Ihr Haus nie
- NGC i.d.R. kein Auftragsverarbeiter
- Kein Drittlandtransfer
- Sie verantworten den sicheren Betrieb
- Vorteil: volle Datenhoheit, leichte DS-Freigabe

Für Betriebsrat & DSB: „Die Gehaltsdaten bleiben im Haus" ist das stärkste Argument — es vereinfacht Zustimmung und Datenschutz-Freigabe spürbar.

Unsere Empfehlung: On-Premise.

Was dafür spricht

- Keine Rolle als Auftragsverarbeiter (kein Datenzugriff)
- Kein Drittlandtransfer, schlankere DSFA
- Einfacheres Vertragswerk (Lizenz statt AVV + SCCs)

Was Sie übernehmen

- Sicherer Betrieb: Server, Backups, Updates
- TOMs in Ihrer Verantwortung (Art. 32)
- Wir liefern Software, Updates & Härtungs-Checkliste

Technische Voraussetzung (ehrlich): Die App läuft heute Cloudflare-nativ. Für On-Premise liefern wir eine portierbare Variante (Container, Standard-DB, lokale Authentifizierung) — damit „keine Daten zu uns" auch technisch hält.

Wenn doch Cloud gewünscht ist

Bleibt die SaaS-Variante voll verfügbar — mit AVV, SCCs und nachgewiesenen Schutzmaßnahmen. **Sie wählen, wir richten beides DSGVO-konform ein.**

Rechte der Mitarbeitenden — erfüllbar.

Auskunft, Berichtigung, Löschung

Erfüllbar über Ihr internes Personalnummer-zu-Pseudonym-Mapping. Wir unterstützen jeden Antrag weisungsgebunden. (Art. 15–22 DSGVO)

Löschkonzept

Definierte Aufbewahrungsfristen (Vorschlag: 3 Jahre Audit-Zeitraum), danach automatische Löschung. Schlüssel-Rotation als „digitales Vergessen".

Für die DS-Prüfung: Speicherbegrenzung (Art. 5 (1) e) und Löschrecht (Art. 17) sind prozessual abgebildet; Report-Dateien folgen derselben Frist über eine Speicher-Lifecycle-Regel.

Zwei Pflichten, bei denen wir zuliefern.

ART. 35 DSGVO

Datenschutz-Folgenabschätzung

Bei systematischer Gehaltsauswertung wahrscheinlich verpflichtend. Wir liefern eine vorbereitete DSFA-Vorlage mit der Risikobewertung.

§ 87 BETRVG

Betriebsrat einbinden

Die Auswertung von Vergütung ist mitbestimmungsnah. Wir liefern die Informations- und Argumentationsgrundlage für die Beteiligung.

Sie bleiben Verantwortlicher

Diese Pflichten liegen beim Arbeitgeber — wir machen Ihnen die Erfüllung mit Vorlagen und Zuarbeit **so leicht wie möglich.**

Datenschutz als Vertrauensvorsprung.

Eingebaut

Pseudonymisierung & Datenminimierung ab Werk — Klarnamen erreichen uns nie.

Ehrlich

Pseudonym ist nicht anonym — wir benennen Grenzen und sichern sie ab.

Rechtssicher

AVV, EU-Hosting, klare Rechtsgrundlage, DSFA-Vorlage.

Sascha Kubak
NextGen Consulting · HR & AI Consulting
sascha.kubak@next-gen-consulting.de

NextGen Consulting

Gerne senden wir AVV & DSFA-Vorlage zu.