KUNDENINFORMATION · DATENSCHUTZ

Datenschutz in der Vergütungsanalyse.

Wie wir die Gehalts- und Personaldaten Ihrer Mitarbeitenden schützen — technisch nachweisbar und rechtlich sauber.

ÜBER DIESES DOKUMENT

Es ist in zwei Ebenen aufgebaut: **Seite 1–2** fassen das Wesentliche für Geschäftsführung und HR zusammen. **Seite 3–4** sind der prüffähige Anhang für Ihre/n Datenschutzbeauftragte/n — mit Rechtsgrundlagen, Maßnahmen und Vertragsbezug.

Das Wichtigste in einem Satz

Die Klarnamen Ihrer Mitarbeitenden verlassen Ihren Browser nie — wir als Betreiber sehen zu keinem Zeitpunkt, wer hinter einer Gehaltszeile steht. Und wir versprechen keine Anonymität, die wir nicht halten können, sondern benennen die Grenzen offen.

Wie der Schutz funktioniert

1

Excel im Browser

Ihre Gehaltsliste wird lokal im Browser eingelesen — nicht hochgeladen.

2

Pseudonym statt Name

Die Personalnummer wird mit einem geheimen Schlüssel zu einem nicht umkehrbaren Code verrechnet.

3

Nur Codes an uns

An unsere Server geht ausschließlich pseudonymisiertes Datenmaterial — keine Namen.

Welche Daten verarbeitet werden

Verarbeitet — pseudonymisiert

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

Bewusst NICHT gespeichert

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

KURZFASSUNG · GESCHÄFTSFÜHRUNG & HR

Ehrlich: Pseudonym ist nicht anonym

Pseudonymisierte Daten gelten rechtlich weiterhin als personenbezogen. In kleinen Gruppen kann die Kombination aus Position, Standort und Geschlecht eine Person erkennbar machen. Wir gehen damit aktiv um:

- Zugriff auf den Schlüssel nur für Import-Berechtigte.
- Auswertungen erst ab einer Mindestgruppengröße ($k \geq 5$) — kleinere Gruppen werden zusammengefasst oder unterdrückt.
- Auswertungen auf Einzelfall-Ebene nur für berechtigte Rollen und protokolliert.

Klare Rollen & ein klarer Vertrag

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

NextGen = Auftragsverarbeiter
Wir verarbeiten ausschließlich weisungsgebunden in Ihrem Auftrag.

AUFTRAGSVERARBEITUNGSVERTRAG
Ein AV-Vertrag (Art. 28 DSGVO) ist verpflichtend — wir stellen ihn inkl. Unterauftragsverarbeiter-Liste und dokumentierter Schutzmaßnahmen bereit.

Rechtsrahmen & Datenstandort

RECHTSGRUNDLAGE

Die **EU-Entgelttransparenzrichtlinie 2023/970** macht das Gender-Pay-Gap-Reporting ab 2026 zur Pflicht. Dazu § 26 BDSG (Beschäftigtenkontext) und berechtigtes Interesse an fairer Vergütung.

DATENSTANDORT

Betrieb mit **aktiver EU-Datenresidenz** auf Cloudflare. Die Daten ruhen in europäischen Rechenzentren; der Drittland-Restpunkt ist über Standardvertragsklauseln abgesichert.

Betriebsmodell: SaaS oder On-Premise

OPTION A · SAAS / CLOUD

NGC betreibt es. NGC ist Auftragsverarbeiter (AVV nötig), Daten liegen bei uns auf Cloudflare (EU-Residenz), Drittland über SCCs abgesichert. Vorteil: null Betriebsaufwand für Sie.

OPTION B · ON-PREMISE — EMPFOHLEN

Sie hosten im Haus. Daten verlassen Ihr Haus nie, NGC ist i.d.R. kein Auftragsverarbeiter, kein Drittlandtransfer. Im Gegenzug verantworten Sie den sicheren Betrieb — wir liefern Software, Updates & Härtungs-Checkliste.

EMPFEHLUNG

On-Premise ist datenschutzrechtlich das stärkere Angebot — „die Gehaltsdaten bleiben im Haus" vereinfacht DSB-Freigabe und Betriebsrats-Zustimmung spürbar. Technische Voraussetzung: eine portierbare Variante (Container, Standard-DB, lokale Authentifizierung) statt der heutigen Cloudflare-Bindung.

Was wir Ihnen abnehmen

PFLICHT DES ARBEITGEBERS	UNSERE ZUARBEIT
Datenschutz-Folgenabschätzung (Art. 35)	Vorbereitete DSFA-Vorlage inkl. Risikobewertung
Betriebsrat-Beteiligung (§ 87 BetrVG)	Informations- und Argumentationsgrundlage
Betroffenenrechte (Art. 15–22)	Weisungsgebundene Unterstützung bei jedem Antrag
Löschkonzept (Art. 5 / 17)	Fristen + automatisierte Löschung, „digitales Vergessen"

Datenschutz als Vertrauensvorsprung

Eingebaut statt aufgesetzt, ehrlich in den Grenzen, rechtssicher im Rahmen — so wird die Pflicht ab 2026 zum Vorteil.

ANHANG · FÜR DATENSCHUTZBEAUFTRAGTE

Prüffähiger Anhang.

Rechtsgrundlagen, technische und organisatorische Maßnahmen und Vertragsbezug für die datenschutzrechtliche Freigabe.

1 · Rollen & Verarbeitung (Art. 28, 30)

ROLLE	AKTEUR	BEMERKUNG
Verantwortlicher	Kunde (Arbeitgeber)	Bestimmt Zwecke & Mittel
Auftragsverarbeiter	NextGen Consulting	Weisungsgebunden, AVV nach Art. 28
Unterauftragsverarbeiter	Cloudflare, Inc.	Hosting; EU-Datenresidenz aktiv

ABHÄNGIG VOM BETRIEBSMODELL

Diese Tabelle gilt für den **SaaS-Betrieb**. Bei **On-Premise** (Hosting beim Kunden ohne NGC-Datenzugriff) ist NGC **kein** Auftragsverarbeiter — der AVV entfällt (außer eng begrenzt für Support-Fernzugriff), ebenso der Cloudflare-/Drittlandbezug.

2 · Datenkategorien

DATUM	EINORDNUNG
Pseudonym (Mitarbeiter & Manager)	SHA-256(Salt + Pers.-Nr.); kein Klarname
Geschlecht	Zweckgebunden auf Pay-Gap-Analyse (keine Art.-9-Verarbeitung)
Geburtsjahr, Eintrittsjahr	Personenbezogen; Re-ID-relevant in kleinen Gruppen
Gehalt, Bonus, FTE, Wochenstunden	Kernzweck; faktisch hochsensibel
Position, Level, Abteilung, Standort	Organisatorisch; in Kombination re-identifizierend
Audit-Log: User-ID, IP-Hash, User-Agent	App-Nutzer (HR); IP nur gehasht gespeichert

3 · Rechtsgrundlagen

- **Art. 6 (1) c DSGVO** i. V. m. EU-Richtlinie 2023/970 / Entgelttransparenzgesetz — rechtliche Verpflichtung (Umsetzung 06/2026).
- **§ 26 BDSG** — Verarbeitung im Beschäftigungskontext.
- **Art. 6 (1) f DSGVO** — berechtigtes Interesse an diskriminierungsfreier Vergütung (mit Abwägung).

4 · Technische & organisatorische Maßnahmen (Art. 32)

Datenminimierung & Pseudonymisierung

- Client-seitiges Hashing; Roh-Excel wird nicht serverseitig gespeichert
- Strict-Schema weist Klarnamen-Felder (name, email, manager) ab
- Eigener Salt je Mandant — keine mandantenübergreifende Verkettung

Integrität & Nachweisbarkeit

- Append-only Audit-Log mit gehashter IP
- Unveränderbare, gelockte Snapshots (Stichtage)
- PDF-Reports mit SHA-256-Prüfsumme für Re-Audit
- Rollenbasierter Zugriff (Admin / Kunde)

5 · Re-Identifikation aktiv begrenzt

RESTRISIKO

Pseudonym ≠ anonym (ErwG 26). Re-ID möglich über (a) Salt + Originalliste und (b) Merkmalskombination in kleinen Gruppen.

MASSNAHMEN

Salt-Auslieferung auf Import-berechtigte Rolle beschränkt · Mindestgruppengröße **k ≥ 5** vor Aggregat-Anzeige · Einzelfall-Auswertung rollenbeschränkt und protokolliert.

6 · Drittland, Aufbewahrung, Betroffenenrechte

Drittland (Art. 44 ff.)	EU-Datenresidenz aktiv; Cloudflare als US-Konzern über SCCs + Transfer-Impact-Assessment im AVV abgesichert.
Aufbewahrung (Art. 5 1e)	Fristbasiert (Vorschlag 3 Jahre Audit-Zeitraum), danach automatisierte Löschung; R2-Reports über Lifecycle-Regel.
Löschung (Art. 17)	Über Pers.-Nr.→Pseudonym-Mapping des Verantwortlichen; Salt-Rotation entkoppelt sämtliche Pseudonyme.
Betroffenenrechte (15–22)	Verantwortlicher erfüllt; NextGen unterstützt weisungsgebunden. Prozess im AVV.
DSFA (Art. 35)	Wahrscheinlich verpflichtend; Vorlage wird bereitgestellt.

Offene Härtungspunkte (Transparenz)

Salt-Zugriff weiter einschränken · k-Anonymität technisch erzwingen · Löschkonzept + R2-Lifecycle finalisieren · DSFA-/AVV-Vorlagen abschließen. Diese Punkte sind dokumentiert und im Backlog priorisiert.

Kontakt: Sascha Kubak · sascha.kubak@next-gen-consulting.de · NextGen Consulting · HR & AI Consulting. Dieses Dokument beschreibt den konzeptionellen Stand und ersetzt keine individuelle Rechtsberatung.