INTERNE DATA PROTECTION POLICY
Converate
Laatst bijgewerkt: 01-03-2025

---

1. Inleiding

Deze **Interne Data Protection Policy** (DPP) is opgesteld om te waarborgen dat Converate voldoet aan de **Algemene Verordening Gegevensbescherming (AVG)** en andere relevante wet- en regelgeving met betrekking tot de verwerking en bescherming van persoonsgegevens. Dit beleid biedt een kader voor hoe medewerkers binnen Converate omgaan met persoonsgegevens en beschrijft de procedures rondom databeheer, beveiliging en meldingen van datalekken.

Deze policy is **bindend** voor alle medewerkers en externe partijen die namens Converate persoonsgegevens verwerken.

---

2. Doel en Toepasselijkheid

Deze policy heeft als doel:

- De bescherming van persoonsgegevens binnen Converate te waarborgen.
- Een veilige en compliant werkwijze te garanderen bij het verwerken van persoonsgegevens.
- Richtlijnen te bieden voor medewerkers over hoe persoonsgegevens correct worden verwerkt, opgeslagen en beschermd.
- De procedure bij beveiligingsincidenten en datalekken vast te leggen.
- Het uitvoeren van een **Data Protection Impact Assessment (DPIA)** bij risicovolle verwerkingen om proactief risico's te beoordelen en te mitigeren.

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens binnen Converate, inclusief maar niet beperkt tot gegevens van:

- Klanten
- Medewerkers
- Leveranciers
- Gebruikers van het Converate-platform

---

3. Grondslagen en Principes van Gegevensbescherming

Converate verwerkt persoonsgegevens uitsluitend op basis van de volgende AVG-grondslagen:

- **Toestemming** – Voor verwerking waarvoor expliciete goedkeuring vereist is.
- **Uitvoering van een overeenkomst** – Wanneer verwerking nodig is voor de uitvoering van een contract.
- **Wettelijke verplichting** – Voor verwerking die noodzakelijk is om aan wettelijke eisen te voldoen.
- **Gerechtvaardigd belang** – Waarbij het belang van Converate zwaarder weegt dan de impact op betrokkenen, zoals onderbouwd in een **Legitieme Belangenafweging (LIA)**. Dit document is te vinden in het privacybeleid van Converate

Alle verwerkingen van persoonsgegevens moeten voldoen aan de **zes kernprincipes van de AVG**:

1. **Rechtmatigheid, behoorlijkheid en transparantie**
2. **Doelbeperking**
3. **Dataminimalisatie**
4. **Juistheid**
5. **Opslagbeperking**
6. **Integriteit en vertrouwelijkheid**

---

4. Interne Richtlijnen voor Databeheer

Om naleving van de AVG te waarborgen, gelden de volgende interne richtlijnen:

4.1. Toegang en Beveiliging

- Alleen medewerkers die persoonsgegevens nodig hebben voor hun functie, krijgen toegang.
- Toegang wordt verstrekt op basis van het **least privilege principle** (zo min mogelijk rechten per medewerker).
- Persoonsgegevens worden **versleuteld opgeslagen** en alleen toegankelijk via beveiligde systemen.

- Werken op afstand vereist gebruik van een **beveiligde VPN-verbinding**, **Multi-Factor Authenticatie (MFA)** en uitsluitend **geautoriseerde apparaten** voor toegang tot systemen met persoonsgegevens.

4.2. Bewaartermijnen en Verwijdering

- Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk.
- **Bewaartermijnen per type gegevens:**
    - Identificeerbare klantgegevens: **6 maanden**, daarna anonimisering.
    - Personeelsgegevens: **5 jaar** na uitdiensttreding.
    - Leveranciersgegevens: **7 jaar** voor boekhoudkundige verplichtingen.
- Na de bewaartermijn worden gegevens automatisch verwijderd of geanonimiseerd.

4.3. Gebruik van Externe Verwerkers

- Externe partijen die namens Converate persoonsgegevens verwerken, moeten een **Verwerkersovereenkomst (DPA)** ondertekenen.
- Gegevens worden primair verwerkt binnen de **Europese Economische Ruimte (EER)**. Indien gegevens buiten de EER worden opgeslagen, worden **Standard Contractual Clauses (SCC's)** toegepast om AVG-conformiteit te waarborgen.
- Halfjaarlijkse interne audits controleren of externe verwerkers voldoen aan de beveiligingsstandaarden van Converate.

---

5. Beveiliging en Preventie van Incidenten

Converate past de volgende beveiligingsmaatregelen toe:

- **Technische maatregelen:** Encryptie, firewalls, multi-factor authenticatie en regelmatige beveiligingsupdates.
- **Organisatorische maatregelen:** Toegangscontroles, geheimhoudingsverklaringen voor medewerkers en periodieke security audits.
- **Logging en Monitoring:** Systemen worden continu gemonitord om ongeautoriseerde toegang of verdachte activiteiten te detecteren.
- **Intern auditsysteem:** Halfjaarlijks worden nalevingsaudits uitgevoerd om AVG-conformiteit te waarborgen.

---

6. Datalekprocedure

Indien er een (vermoedelijk) datalek plaatsvindt, moet dit onmiddellijk worden gemeld bij de **Data Protection Officer (DPO)**. Een datalek omvat:

- Verlies of diefstal van persoonsgegevens.
- Ongeautoriseerde toegang tot gegevens.
- Onbedoelde openbaarmaking van persoonsgegevens door medewerkers.

6.1. Meldprocedure

1. **Direct melden**: Medewerkers melden een (mogelijk) datalek direct aan de DPO via contact@converate.nl.
2. **Onderzoek en documentatie**: De DPO onderzoekt de ernst van het incident en documenteert:
    - Wat er is gebeurd?
    - Welke persoonsgegevens betroffen zijn?
    - Hoe het lek is ontstaan?
    - Welke maatregelen al zijn genomen?
3. **Meldplicht Autoriteit Persoonsgegevens (AP)**: Indien er sprake is van risico's voor betrokkenen, wordt het lek binnen **72 uur** gemeld aan de AP.
4. **Communicatie met betrokkenen**: Indien nodig worden getroffen personen geïnformeerd over het datalek.
5. **Nazorg en preventie**: Het incident wordt geëvalueerd en waar nodig worden preventieve maatregelen genomen.

---

7. Handhaving en Sancties

- Overtredingen van deze policy kunnen leiden tot disciplinaire maatregelen, waaronder waarschuwingen, schorsingen of beëindiging van het dienstverband.
- Ernstige overtredingen kunnen leiden tot juridische stappen.
- Medewerkers krijgen **verplichte jaarlijkse AVG-trainingen** om compliance en bewustzijn te vergroten.

---

8. Wijzigingen en Evaluatie

Deze Data Protection Policy wordt **jaarlijks geëvalueerd** en indien nodig geüpdatet om te voldoen aan nieuwe wet- en regelgeving en technologische ontwikkelingen.

De meest recente versie is altijd beschikbaar voor medewerkers via het interne documentatiesysteem.

---

9. Contactinformatie

Voor vragen over dit beleid of datalekmeldingen kunt u contact opnemen met: **Data Protection Officer (DPO) – Converate**
contact@converate.nl
de brauwweg 52-66, 3125AE, Schiedam
0618447819

Deze interne Data Protection Policy is bindend voor alle medewerkers van Converate en moet strikt worden nageleefd om te voldoen aan de AVG en andere toepasselijke regelgeving.