Interne Richtlijn: Eigenaarschap, Opslag en Gebruik van Gegevens uit Klantinteracties

1. Doel en Reikwijdte

Deze richtlijn beschrijft hoe medewerkers moeten omgaan met gegevens die voortkomen uit klantinteracties, waaronder telefoongesprekken, e-mails, chats, formulieren, social media-contacten en andere communicatiemiddelen. De richtlijn geldt voor alle medewerkers, tijdelijke krachten en externe partijen die namens de organisatie met klantdata werken.

2. Uitgangspunten

2.1 Klant als eigenaar

- Persoonsgegevens die voortkomen uit klantinteracties zijn eigendom van de klant.
- De organisatie beheert deze gegevens uitsluitend om dienstverlening te kunnen leveren en te verbeteren.

2.2 Vertrouwelijkheid

- Alle klantgegevens worden vertrouwelijk behandeld.
- Medewerkers krijgen alleen toegang tot gegevens indien dit noodzakelijk is voor hun functie (need-to-know-principe).

3. Verzamelen van gegevens

3.1 Transparantie

- Klanten worden duidelijk geïnformeerd over welke gegevens worden verzameld, voor welk doel, hoe lang gegevens worden bewaard en hun rechten onder de AVG.

3.2 Data minimalisatie

- Er worden alleen gegevens verzameld die noodzakelijk zijn voor het uitvoeren van de dienstverlening of wettelijke verplichtingen.
- Onnodige of dubbele gegevens worden niet opgeslagen of direct verwijderd.

4. Opslag en Beveiliging

4.1 Beveiligingsnormen

- Gegevens worden opgeslagen volgens geldende beveiligingsstandaarden (bijv. ISO 27001 of sectorale equivalenten).
- Encryptie is verplicht tijdens opslag en verzending.

4.2 Locatie van opslag

- Opslag vindt plaats binnen de EU of in EER systemen die voldoen aan AVG-vereisten.
- Cloudleveranciers dienen een geldige verwerkersovereenkomst te hebben.

4.3 Bewaartermijnen

- Per type klantinteractie gelden vooraf vastgestelde bewaartermijnen.
- Na het verstrijken van de termijn worden gegevens veilig verwijderd of geanonimiseerd.

5. Gebruik van gegevens

5.1 Doelbinding

- Gegevens worden uitsluitend gebruikt voor het doel waarvoor ze zijn verzameld.
- Voor afwijkend gebruik (zoals training van AI-modellen, marketing of profilering) is expliciete toestemming van de klant nodig.

5.2 Anonimisering

- Analyses, rapportages en kwaliteitsmetingen worden bij voorkeur uitgevoerd op geanonimiseerde datasets.
- Wanneer volledige anonimisering niet mogelijk is, wordt pseudonimisering toegepast.

5.3 Interne toegang

- Medewerkers mogen gegevens alleen gebruiken wanneer dit noodzakelijk is voor hun werkzaamheden.
- Gebruik wordt gelogd en kan worden gecontroleerd via periodieke audits.

6. Delen van gegevens

6.1 Externe partijen

- Gegevens worden uitsluitend gedeeld met externe partijen wanneer dit noodzakelijk is en een verwerkersovereenkomst is afgesloten.
- Externe partijen moeten werken volgens dezelfde beveiligings- en privacy-eisen.

6.2 Geen ongeautoriseerde verstrekking

- Gegevens worden nooit gedeeld met derden zonder wettelijke grondslag of expliciete toestemming van de klant.

7. Governance en Verantwoordelijkheden

7.1 Rollen

- Data Protection Officer (DPO): Adviseert over privacywetgeving en bewaakt naleving.
- Proceseigenaren / afdelingsmanagers: Verantwoordelijk voor correcte toepassing binnen hun teams.
- Alle medewerkers: Verantwoordelijk voor het veilig en zorgvuldig omgaan met klantdata.

7.2 Periodieke controles

- Jaarlijks worden audits uitgevoerd op naleving van deze richtlijn.
- Bevindingen worden gerapporteerd aan het management en opgevolgd.

7.3 Incidentprocedure

- Vermoede of daadwerkelijke datalekken worden onmiddellijk gemeld volgens de interne incident- en escalatieprocedure.
- Indien nodig worden klanten geïnformeerd conform de AVG.

8. Ethische gedragsregels

8.1 Respectvolle omgang met klantdata

- Klantgegevens worden gebruikt met respect voor privacy en met aandacht voor de impact op de klant.

8.2 Geen misbruik

- Data mag niet worden gebruikt voor discriminatie, ongewenste beïnvloeding of andere niet-ethische doeleinden.

8.3 Menselijke controle bij automatisering

- Geautomatiseerde besluitvorming wordt altijd aangevuld met menselijke beoordeling.

9. Handhaving

- Niet-naleving van deze richtlijn kan leiden tot disciplinaire maatregelen, waaronder intrekking van toegang, melding aan HR of andere passende stappen volgens het interne reglement.