Ethisch kader

Robuust en veilig

1. Passende cybersecurity
2. Toepassing van zelflerende systemen altijd binnen vooropgestelde kaders
2. Technische problemen zo spoedig mogelijk oplossen
4. Continue monitoring datasystemen
5. Datakwaliteit is adequaat
6. Weloverwogen keuze bij toepassen van o.a. biometrie/social media data
7. Data (governance) vast onderdeel van beleid

Privacy

1. Persoonsgegevens conform AVG-vereisten
2. Waar nodig DPIA bij inzet data-toepassingen
3. Dataminimalisatie en/of vergroten privacy (verbeteringstechnieken)
4. Gedegen bescherming (trainings)data
5. Goed opgeleide medewerkers
6. Adequaat menselijk toezicht
7. Nieuwe technieken eerst testen in vertrouwde omgeving en vergelijken met oude methode

Menselijke autonomie

1. Voorafgaand adequate compliance beoordeling
2. Onderscheid mens/machine waar nodig

Diversiteit/non-discriminatie

1. Bij ongerechtvaardigde discriminatie geen inzet data-toepassing
2. Bijzondere aandacht voor mensen met een beperking

Transparantie

1. Voorlichting aan klanten op orde
2. Menselijke interventie op elk moment mogelijk en achteraf uitkomsten verantwoorden

Maatschappelijk welzijn

1. Gevolgen voor groepen klanten monitoren
2. Verzekerbaarheid borgen of klanten op alternatief wijzen

Verantwoording

1. Interne controle aanwezig voor systemen en gekozen bronnen
2. Kennis van bestuurders bevorderen
3. Zorgen voor gedegen interne communicatie
4. Risico- en effectbeoordeling voor direct belanghebbenden
5. Bevorderen deskundigheid auditmedewerkers
6. Open cultuur waar ethiek onderdeel van uitmaakt
7. Gemaakte keuzes vastleggen
8. Klanten informeren over klachtmogelijkheid