

8 juli 2025

Diversiteit meten met privacy in balans

Aakriti Bhatia en Paul van der Gun



Opzet van de break-out sessie

1. Wie zijn wij?
2. Introductie
3. Juridisch kader
4. Stap-voor-stap aanpak

Dit zijn wij



Aakriti Bhatia



Paul van der Gun

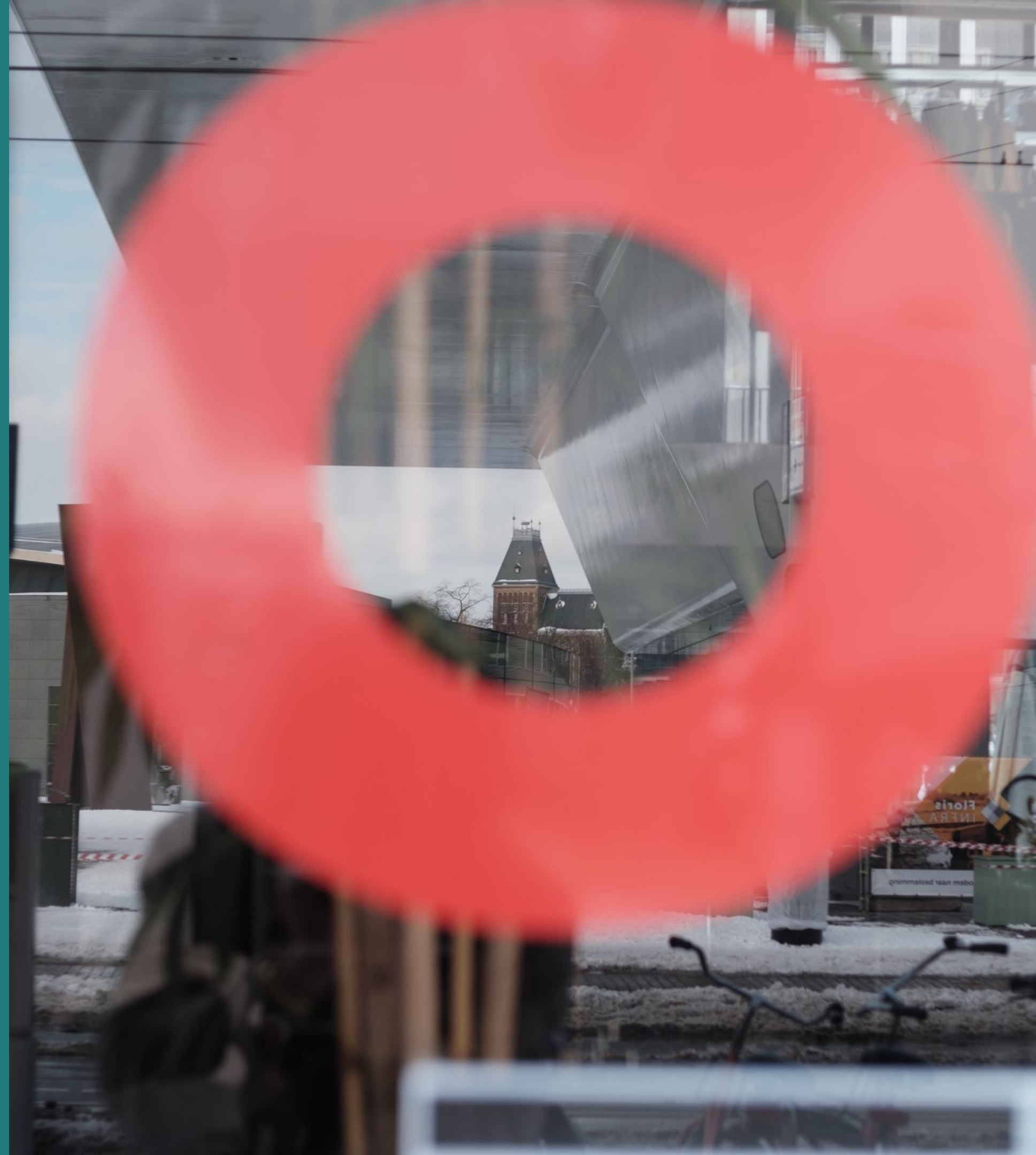


Introductie

- Hoe verzamel je gegevens over diversiteit en inclusie zonder daarbij de AVG te overtreden?
- Meten is weten

**Wie monitort D&I
binnen de
werkomgeving?**

**Wie loopt er wel eens
vast op AVG-
vraagstukken?**



Juridisch kader

- **Persoonsgegevens**

"Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens."

"Een geïdentificeerde of identificeerbare natuurlijke persoon"

"Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

- **Verwerking**

"Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld."

- **Pseudonimisering**

- **Verwerkingsverantwoordelijke**

"Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt."

- **Betrokkenen**

- **Toestemming**

"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."

"Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven. "

- **Inbreuk**

- **Gegevens over gezondheid**

1. **Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
2. **Verwerking:** een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
3. **Pseudonimisering:** het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
4. **Verwerkingsverantwoordelijke:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
5. **Betrokkenen:** Een geïdentificeerde of identificeerbare natuurlijke persoon
6. **Toestemming:** elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.
7. **Inbreuk in verband met persoonsgegevens:** een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
8. **Gegevens over gezondheid:** persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.



Wat is een persoonsgegeven?

Casus: een innovatieve juwelier heeft een chip ontwikkeld die in gouden, met diamant belegde ringen 'verstopt' kan worden. Aan de buitenkant zie je niets, maar met behulp van de chip kan de eigenaar via een app realtime de locatie volgen. Handig als de ring wordt gestolen of kwijtraakt. Maar uiteraard niet geheel zonder privacyrisico's.

De techneuten hebben een lijst met gegevens aangeleverd met de vraag of je aan kunt geven welke van deze gegevens persoonsgegevens zijn. Dat is van belang omdat er uiteraard in lijn met de AVG gewerkt moet worden en er plannen zijn om een grote hoeveelheid slimme ringen te verkopen.

Soorten persoonsgegevens

Reguliere persoonsgegevens:

Gegevens die iemand kunnen identificeren, maar niet gevoelig van aard zijn. Denk aan naam, adres, geboortedatum, telefoonnummer of nationaliteit (in veel gevallen).

Let op: gebruik je nationaliteit om onderscheid te maken op basis van etnische afkomst kwalificeert het als bijzonder persoonsgegeven

Bijzondere persoonsgegevens

Gegevens die extra gevoelig zijn vanwege het risico op discriminatie of misbruik. De AVG noemt expliciet: gegevens over ras of etnische afkomst, politieke opvattingen, religie of levensovertuiging, vakbondslidmaatschap, genetische gegevens, biometrische gegevens (voor identificatie), gezondheid, seksuele leven of seksuele gerichtheid.

Welke van de onderstaande gegevens die gebruikt worden bij de slimme ring zijn persoonsgegevens?

1. Locatiegegevens van de ring
2. Naam van de eigenaar
3. Gewicht van de ring
4. Hoeveelheid diamanten
5. Inloggegevens van de app
6. Uniek serienummer van de chip



Beginnelsen van de AVG

1. **Rechtmatigheid, behoorlijk en transparant:** Persoonsgegevens moeten op een wettelijke, eerlijke en transparante manier worden verwerkt.
2. **Doelbinding:** Gegevens mogen alleen worden verzameld voor uitdrukkelijk omschreven, gerechtvaardigde doelen.
3. **Minimale gegevensverwerking:** Alleen de persoonsgegevens die noodzakelijk zijn voor het beoogde doel mogen worden verzameld en verwerkt.
4. **Juistheid:** De verwerkte persoonsgegevens moeten juist en actueel zijn.
5. **Opslagbeperking:** Gegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor ze zijn verzameld.
6. **Integriteit en vertrouwelijkheid:** Persoonsgegevens moeten goed worden beveiligd

Grondslagen en uitzonderingsgronden

Reguliere persoonsgegevens mogen alleen worden verwerkt als daarvoor een geldige grondslag bestaat.

Er zijn zes wettelijke grondslagen, waarvan in het kader van D&I-beleid met name twee van belang kunnen zijn:

- Toestemming
- Gerechtvaardigd belang

De verwerking van **bijzondere persoonsgegevens** is in principe verboden, tenzij een uitzondering van toepassing is.

Er zijn 10 uitzonderingsgronden, waarvan in het kader van D&I-beleid er één van belang is:

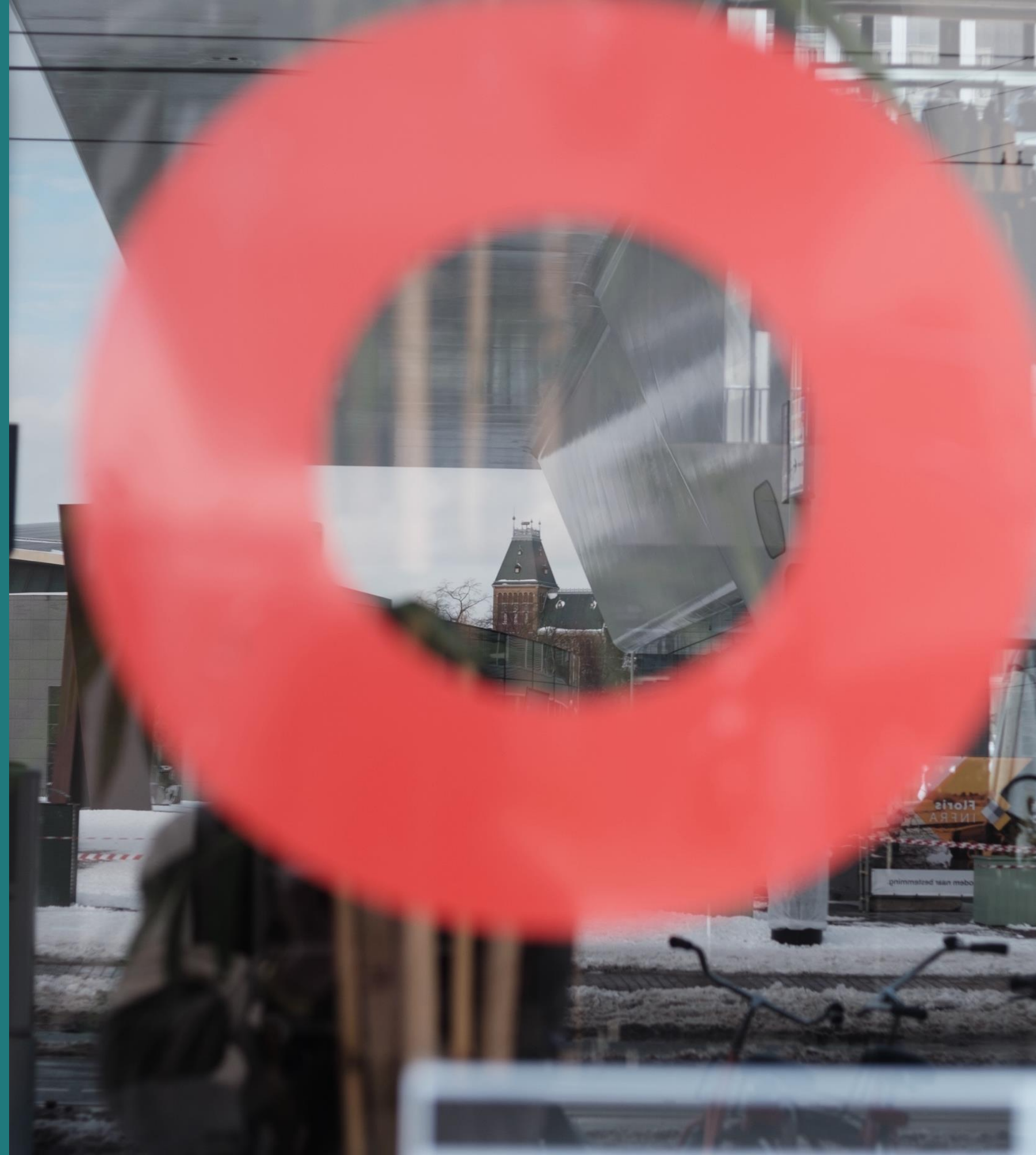
- Expliciete toestemming

Anonimiseren

Pseudonimiseren

Aggregeren

Let op de uitvoering! Echte anonimiteit vereist een strakke aanpak.



Oefening: anoniem of pseudoniem?

Zin A:

In een dataset zijn alle namen vervangen door unieke nummers. Slechts één HR-medewerker heeft toegang tot het document waarin staat welk nummer bij welke medewerker hoort.

Zin B:

Een bedrijf publiceert de resultaten van een enquête, uitgesplitst per team van 3 medewerkers, zonder verdere identificatie. Binnen het bedrijf is echter bekend wie in welk team zit.

Zin C:

Een externe partij ontvangt alleen geaggregeerde data (bijvoorbeeld: "25% van de medewerkers ervaart discriminatie"), zonder toegang tot onderliggende ruwe data.

Zin D:

In een onderzoek naar inclusie zijn alle persoonsgegevens verwijderd, behalve geboortedatum, geslacht en afdeling. De data worden opgeslagen in een versleuteld bestand zonder sleutel.

Rechten van werknemers in het kader van D&I onderzoek

1. Recht op informatie
2. Recht op inzage
3. Recht op rectificatie
4. Recht op gegevenswissing (niet onbeperkt)
5. Recht op beperking van verwerking
6. Recht van bezwaar (bij grondslag gerechtvaardigd belang)



Oefening:

1. Juist of onjuist: Als een werknemer toestemming geeft voor deelname aan een D&I-enquête, mag de organisatie deze gegevens blijven bewaren.
2. Een medewerker krijgt een enquête voorgelegd waarin gevraagd wordt naar zijn seksuele oriëntatie, zonder verdere uitleg over het doel of gebruik van de gegevens. Welke rechten of beginselen worden hier vermoedelijk geschonden?

(Meerdere antwoorden mogelijk)

- A. Recht op informatie
- B. Recht op beperking van verwerking
- C. Het beginsel rechtmatigheid
- D. Het beginsel opslagbeperking

Praktische aanpak: hoe doe je het goed?

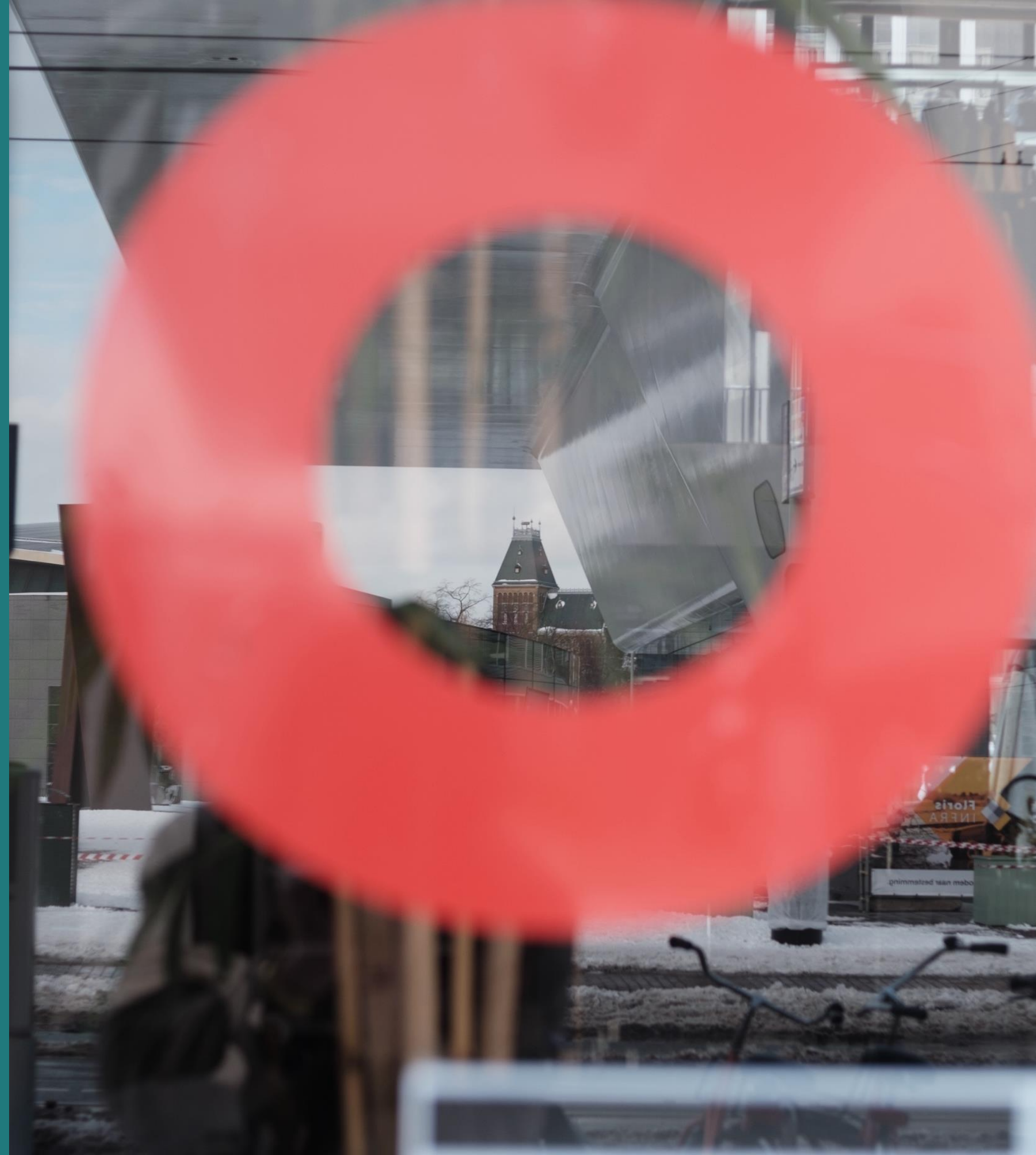
Stap 1: bepaal het doel

Denk aan vragen als:

- Waarom wil je het doen?
- Wat wil je er mee bereiken?

Denk aan antwoorden als:

- Het in kaart brengen van de samenstelling van het personeelsbestand.
- Het constateren van verschillen en deze kleiner maken.



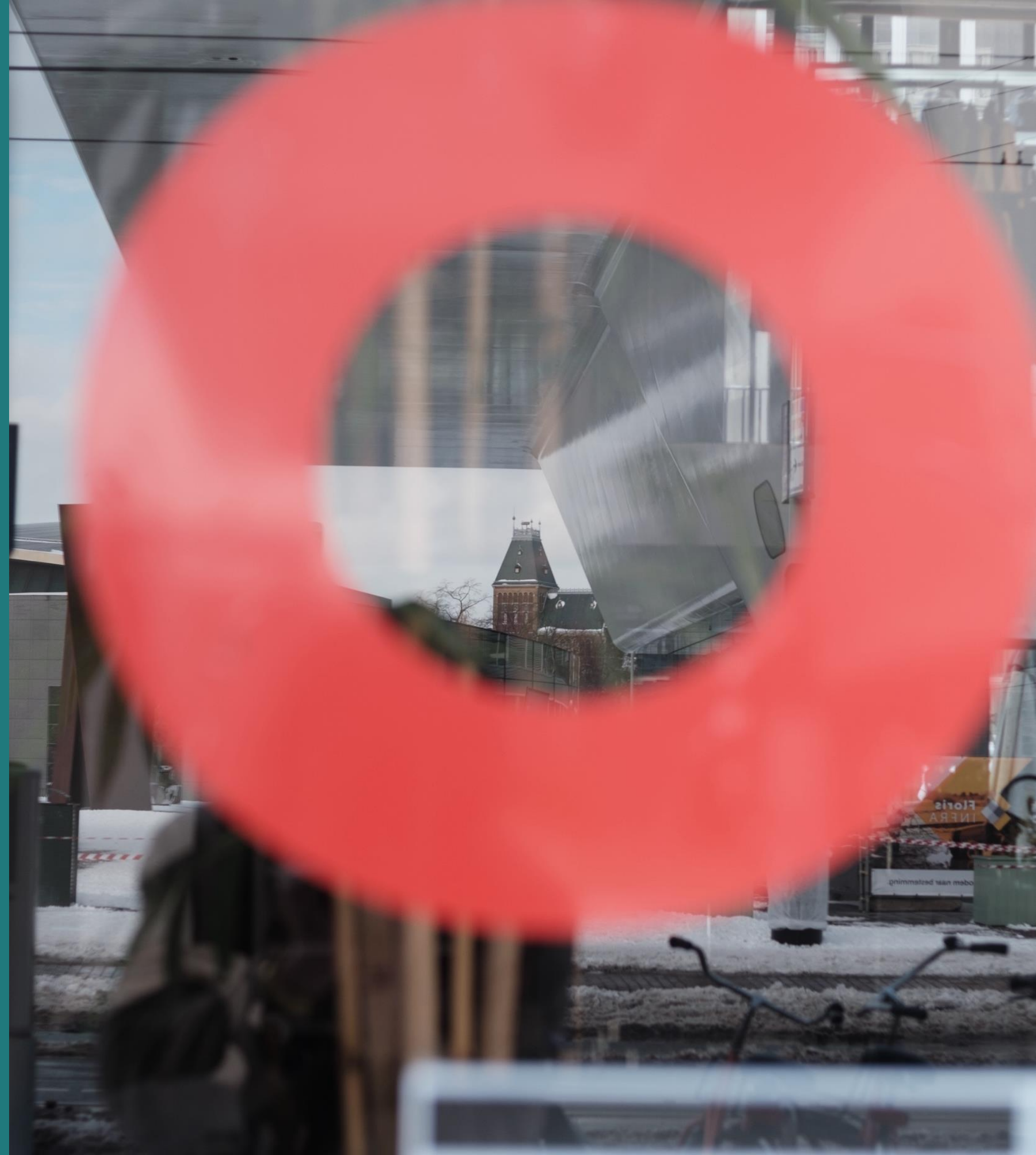
Stap 2: kies een grondslag

Is toestemming haalbaar?

Heb je je gerechtvaardigd belang uitgewerkt?

Denk aan antwoorden als:

- Het in kaart brengen van de samenstelling van het personeelsbestand.
- Het constateren van verschillen en deze kleiner maken.





Stap 3: anoniem of pseudoniem

Toestemming vragen aan werknemers blijkt in praktijk lastig

Stap 4: Zorg voor een duidelijke informatievoorziening

Geef in begrijpelijke taal aan je werknemers aan:

- Wat het doel is van het onderzoek;
- Welke gegevens worden verzameld;
- Hoe lang de gegevens worden bewaard;
- Wie eventueel toegang heeft tot de gegevens;
- Dat deelname niet verplicht is.

Dit kun je doen via een begeleidende e-mail, toelichting in het onderzoek zelf of in een privacyverklaring.



Stap 5: Formuleer zorgvuldige en niet-stigmatiserende vragen

Formuleer inclusievragen neutraal en respectvol. Denk aan vragen over:

- Beleving van inclusie of uitsluiting;
- Ervaringen met discriminatie, pestgedrag of ongelijk behandelen;
- Of medewerkers zich veilig voelen en zichzelf kunnen zijn;
- Het gedrag van collega's, leidinggevenden of klanten.

Koppel dit aan vrijwillige zelfidentificatievragen over gender, leeftijd, etnisch-culturele achtergrond, arbeidsbeperking of seksuele oriëntatie.



Stap 6: Beperk toegang en beveilig alles goed

Ben je ervan bewust dat elke tool die je kiest risico met zich meebrengt!

Aandachtspunten:

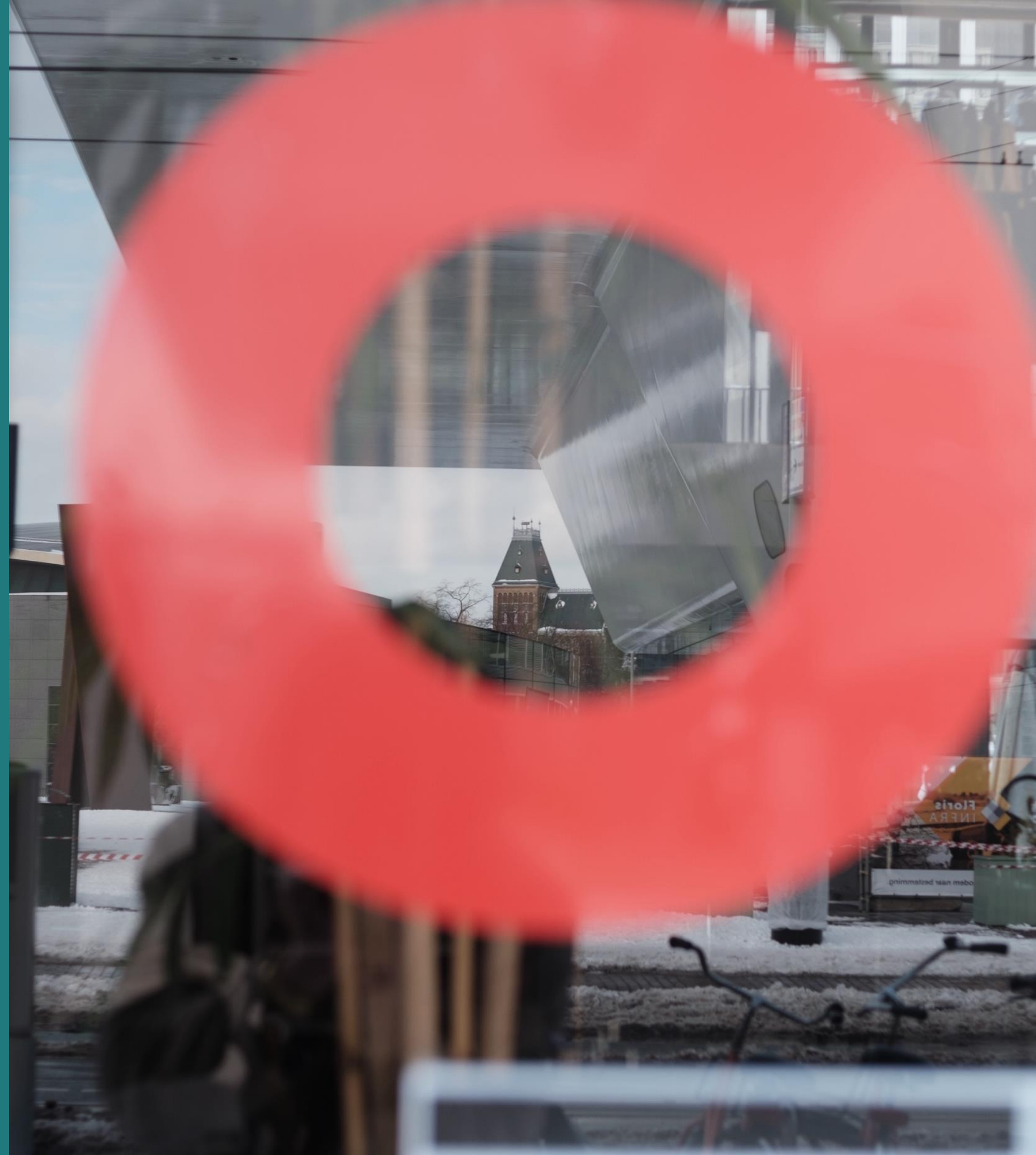
- Goede autorisatie en beperkte toegang;
- Sla gegevens op binnen de EER;
- Verwijder data die je niet nodig hebt;
- Voorkom dat reportages herleidbaar zijn.

Stap 7: Koppel resultaten terug en ondernem actie

Transparantie is cruciaal.

- Wat gebeurt er met de resultaten?
- Welke acties en beleidsmaatregelen worden er genomen?
- Wanneer en hoe vindt herhaling plaats van het onderzoek?

Hiermee vergroot je het vertrouwen en het draagvlak voor D&I beleid.



Stap 8: Evalueer periodiek en stel bij

D&I (en privacy) is geen eenmalige exercitie.

Evalueer:

- Of je vragenlijst en verwerkingswijze nog in lijn zijn met de AVG;
- Of je draagvalk toe- of afneemt;
- Of je acties effect hebben;
- Of een nieuwe evaluatie wenselijk is.

Zorg dat zowel inclusie als je privacybescherming geen papieren doel blijven. Maak ze onderdeel van je beleid én praktijk.



Oefenvragen: goed of fout?

- In hoeverre voelt u zich geaccepteerd binnen uw team, ongeacht uw achtergrond of identiteit?
- Heeft u in de afgelopen 12 maanden op de werkvloer discriminatie, uitsluiting of pestgedrag ervaren of waargenomen?
- Vul hieronder uw leeftijd, afdeling en migratieachtergrond in om ons te helpen D&I-patronen te herkennen:
- Heeft u een arbeidsbeperking of langdurige aandoening waar de organisatie rekening mee moet houden in het D&I-beleid?
- Ervaart u dat leidinggevenden inclusief gedrag vertonen (bijvoorbeeld: gelijke behandeling, ruimte voor diversiteit van meningen en achtergronden)?

Vragen?



ICTRECHT

Stel ze gerust of stuur ze ons:

a.bhatia@ictrecht.nl

p.vandergun@ictrecht.nl



Bedankt!