Gemeente Amsterdam

Opdrachtformulering

project	**Inrichten (basis) compliance bij Bureau Inclusie & Diversiteit**
datum	13-08- 2025
opdrachtgever	**Ambtelijk** 5.1, 2, e
projectleider	5.1, 2, e e
opsteller	5.1, 2, e e
startdatum	1 oktober 2025
einddatum	1 april 2026
versie	0.2
status	intern concept / ~~ambtelijk concept / bestuurlijk concept / ambtelijk vastgesteld / bestuurlijk vastgesteld~~
gevraagd besluit	Ambtelijke goedkeuring voor de start van het project.
vraag	Hoe richten we de (basis) compliance in binnen Bureau Inclusie & Diversiteit?
achtergrond	Voorheen viel het programma Inclusie & Diversiteit organisatorisch onder de directie P&O. Het GMT heeft medio 2023 besloten om het programma Inclusie & Diversiteit te verduurzamen in een Bureau (Bureaunotitie, 4 juli 2023). Met ingang van 1 januari 2024 is dit geformaliseerd.
probleemstelling	De overgang van een programma naar een Bureau betekent een transitie van tijdelijke werkzaamheden naar het inrichten van structurele (werk)processen en routines binnen een duurzame bureauorganisatie. Waar het programma voorheen onderdeel uitmaakte van de directie P&O en voor veel zaken kon meeliften, is dat nu niet meer het geval. Elk organisatieonderdeel moet zijn eigen compliance inrichten. Dit betekent wat we moeten werken in overeenstemming met de geldende wet- en regelgeving (AVG, Archiefwet, Woo, normenkaders zoals de Baseline Informatiebeveiliging Overheid (BIO). Specifiek gaat het om: **Informatiebeheer**. Dit omvat alle activiteiten die nodig zijn om ervoor te zorgen dat informatie toegankelijk, betrouwbaar, relevant en bruikbaar is. Het gaat om processen en procedures voor het maken, opslaan, gebruiken, delen, archiveren en vernietigen van informatie.

Gemeente Amsterdam

Informatiebeveiliging. Gaat in de kern over het beschermen van alle door het Bureau Inclusie & Diversiteit gebruikte informatie op basis van de principes van informatiebeveiliging: *beschikbaarheid, vertrouwelijkheid en integriteit* in lijn met geldende wet en regelgeving zoals BIO 2.0, CBW

Privacy (gegevensbescherming). Dit heeft betrekking op de rechten van individuen met betrekking tot hun persoonsgegevens en de manier waarop deze gegevens worden verwerkt. De Algemene Verordening Gegevensbescherming (AVG) is een belangrijke wet die o.a. regels stelt aan de verwerking van persoonsgegevens. De AVG vereist dat we transparant zijn over de manier waarop we persoonsgegevens verwerken.

doel

1. Zorgen dat we binnen Bureau I&D werken in overeenstemming met de geldende wet- en regelgeving (compliance). Specifiek met betrekking tot informatiebeheer, informatiebeveiliging en privacy. Het gaat om wetten en regels van de Rijksoverheid maar ook om de normen, principes en regelgeving van de gemeente Amsterdam zelf.
2. Bevorderen van een cultuur van compliance (compliance awareness). Compliance is een continu proces en een integraal onderdeel van de werkwijze binnen het Bureau I&D.
3. Bevorderen van een cultuur van risico-gestuurd denken en praten. Bij steeds meer wetgeving wordt uitgegaan dat organisaties risico methodieken hanteren in het toepassen ervan binnen processen.

resultaat

Voor **informatiebeveiliging** is het resultaat dat we voldoen aan de BIO 2.0 (Baseline Informatiebeveiliging Overheid). We hebben de 5 stappen doorlopen om aan te kunnen tonen dat wij ‘in control’ zijn en de juiste maatregelen nemen om BIO-compliant te worden. Dit betekent o.a. dat we een aantal beheersmaatregelen moeten implementeren. En dat we een informatiebeveiligingsplan opstellen en uitvoeren. Hierin staan o.a. verbeteracties geprioriteerd en aangegeven welke verbeteringen bijvoorbeeld binnen 3, 6 of 9 maanden worden doorgevoerd.

Voor **informatiebeheer** is het resultaat dat onze documenten en dossiers
voldoen aan verschillende wet- en regelgeving, waaronder de Archiefwet, AVG en Wet open overheid (Woo). Dit betekent o.a. dat, na migratie van de G-schijf naar MS teams, onze informatie goed geordend is in duidelijke structuren. En dat bestanden en informatie

op tijd worden vernietigd, of worden bewaard in het Stadsarchief. Bij het (samen)werken in MS teams werken we volgens de module Werkafspraken & Inrichting . Hier besteden we ook aandacht aan informatiebeveiligingselementen.

Informatie moet goed vindbaar en te beheren zijn. Om de terugvindbaarheid van informatie te vergroten (bijvoorbeeld voor een Woo verzoek) maken we in het team afspraken over duidelijke naamgeving (o.a. padlengte, versienummering), wie verantwoordelijk is voor welk dossier (o.a. verantwoordelijk voor het aanmaken, behandelen, het op orde houden en tijdig afsluiten van het dossier). Zie hierover:
10 Gouden regels voor het beheren van informatie Dit vraagt van alle collega´s een bepaalde tijdsinvestering om te werken binnen de juiste structuur.

Voor **privacy** beschrijven we welke werkprocessen we hebben en per werkproces of en welke persoonsgegevens worden verwerkt, wat er met deze gegevens wordt gedaan, met wie deze worden gedeeld, hoe deze worden beschermd en waar en hoelang deze worden bewaard. Dit nemen we op in het verwerkingsregister. Dit register is verplicht omdat eisen worden gesteld aan het zorgvuldig verwerken van persoonsgegevens en aantoonbaar maken dat de AVG wordt nageleefd.
Verder betrekken we onze privacy officer in een vroeg stadium bij (nieuwe) processen of ingebruikname van applicaties zodat deze worden ingericht conform de AVG vereisten. Het tijdig betrekken van de privacy officer gebeurt ook bij het maken van afspraken met derden. Denk hierbij aan het afsluiten van verwerkings- of leveringsovereenkomsten of het opstellen van DPIA’s (Data Protection Impact Assessment).

Samengevat: bij compliance gaat het erom in kaart te brengen welke (werk) processen we hebben en hoe we deze vertalen naar de geldende regels en voorschriften

afbakening Deze opdrachtformulering heeft betrekking op werkzaamheden die als resultaat hebben het inrichten van de (basis) compliance. De opdrachtformulering gaat niet over het onderhouden, bestendigen en eventuele verbeteracties rond compliance.

geld Werkzaamheden vinden plaats binnen de huidige begroting.

Gemeente Amsterdam

organisatie

Ambtelijk opdrachtgever: 5.1, 2, e

Projectleide 5 5.1, 2, e e

Overige betrokkenen (intern Bureau I&D): alle teamleden.

Overige betrokkenen (extern Bureau I&D): i-lead, een Information Security Officer, van de afdeling Digitale Strategie en Informatie, een Privacy Officer.

tijd

Planning op hoofdlijnen

Wat	Wie	Periode
Opstellen van Plan van Aanpak Gedetailleerde beschrijving van activiteiten om de hierboven genoemde resultaten te bereiken. Het PvA omvat de volgende onderdelen: probleemanalyse, doelstellingen, werkwijze, tijdsplanning, middelen, organisatie (de organisatiestructuur van het project, verantwoordelijkheden en communicatie). Verder risicoanalyse (mogelijke risico's en knelpunten worden	Projectleider *Inzet: 1 dag per week* Input van teamleden, en mogelijk externen (i-lead, een Information Security Officer, een Privacy Officer? *Inzet: PM.*	Okt. 2025

geïdentificeerd en er wordt aangegeven hoe hiermee zal worden omgegaan) en evaluatie (de wijze waarop het project zal worden geëvalueerd en de criteria voor succes worden beschreven).		
Uitvoering PvA	Projectleider *Inzet: 1 dag per week*	1 nov. 2025 tot 1 apr. 2026

informatie De projectleider informeert de opdrachtgever minimaal 1 x per maand over de voortgang. Dat gebeurt aan de hand van het (nog) op te stellen Plan van Aanpak.

kwaliteit Het (eind)resultaat voldoet aan de kwaliteitseisen die intern worden gesteld. Vragen die beantwoord moeten worden om te beoordelen of aan de kwaliteitseisen is voldaan zijn o.a. : hebben we als Bureau de 5 stappen goed doorlopen om BIO compliant te zijn? Voldoen we aan de module Werkafspraken en Inrichting? Hebben we werkafspraken gemaakt over (samen)werken binnen MS teams?

ICT N.v.t.

communicatie/ participatie Teamleden worden via het teamoverleg geïnformeerd over de start van de inrichting van compliance binnen het Bureau en wat van hen hierbij wordt verwacht. Voor het opstellen van het Plan van Aanpak betekent dit in ieder geval een gesprek/interview met alle teamleden om inzicht te krijgen welke werkprocessen bij hun taken horen, of en welke persoonsgegevens worden verwerkt, wat er met deze gegevens wordt gedaan, met wie deze worden gedeeld en of er specifieke applicaties worden gebruikt.

Risico's Voldoen aan compliance betekent een andere manier van (werk)processen inrichten en een andere manier van werken (volgens een andere structuur). Dit houdt een cultuur- en gedragsverandering in, wat tot weerstand kan leiden. (*Waarom moet ik het bestand zo opslaan? Hoezo moet dit anders? We hebben het altijd op deze*

manier gedaan etc.).

Niet (blijvend) naleven van wet- en regelgeving kan juridische gevolgen hebben. Dit kan leiden tot boetes of andere juridische maatregelen.

Capaciteit. De projectleider moet voor het opstellen van en uitvoeren van het PvA voldoende tijd beschikbaar te hebben. Als de projectleider meer taken heeft dan beschikbare capaciteit zal de opdrachtgever prioriteiten moeten stellen. Dit kan gevolgen hebben voor de tijdsplanning.

akkoord opdrachtgever

plaats

datum

akkoord projectleider

plaats

datum