Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Aan de Stedelijk Directeur Sociaal, de heer E. Ten Hulsen, de Directeur Inkomen, de heer H. Aalders en de heer 5.1 5.1, 2, e , manager IV Sociaal
C.c. de CIO, de heer J. Flippo,
C.c. de heer 5.1, 5.1, 2, e , privacy coördinator Cluster Sociaal

Datum	U 17020
Ons kenmerk	23 februari 2017
Behandeld door	Mw. 5.1, 2, e
Doorkiesnummer	5.1, 2, e
Faxnummer	nvt
E-mail	5.1, 2, e @amsterdam.nl
Bijlage	1
Onderwerp	Advies Commissie Persoonsgegevens Amsterdam

Geachte heren,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 26 januari 2017 waren namens de gemeente Amsterdam aanwezig: de heer 5.1 5.1, 2, e (teammanager PIM, IV Sociaal) en mr. 5.1, 5.1, 2, e (privacy coördinator Cluster Sociaal). Namens Wigo4it waren aanwezig: de heer 5.1, 2, e (directiesecretaris), de heer 5.1, 2, e 5.1, 2, e (adjunct-directeur).

Bij het besloten agendapunt "Wigo4it" is het volgende besproken.

Op 14 november 2015 heeft een gesprek plaatsgevonden met de CPA, de directie van Wigo4it en de security officer van Wigo4it. Daarbij is toen gesproken over de organisatie van Wigo4it, het verbeterplan voor de processen, de jaarlijkse audit en het security management van de systemen. Het "Assurance-Rapport inzake opzet, bestaan en werking van General IT-Controls bij Wigo4it in 2015" is daarop, zonder het "in control statement", eerst op de vergadering van 10 november 2016 als ingekomen stuk aangeleverd en besproken.
De CPA vindt dat het aanleveren van het rapport te lang op zich heeft laten wachten en wijst er op dat het "in control statement" nog steeds ontbreekt.

Daarop is op uitnodiging van de CPA op 26 januari 2017 inhoudelijk van gedachten gewisseld over het Assurancerapport 2015, de voortgang van de verbetering van de processen, het security management en het access management.

Vanwege uw verantwoordelijkheid voor Wigo4it informeren we u bij deze over de afspraken die de CPA met Wigo4it gemaakt heeft.

Allereerst onderschrijft de CPA het 'oordeel met beperking' en de daaruit voorkomende aandachtspunten uit het eerdergenoemde rapport. De CPA acht daarbij met name van belang dat Wigo4it op het gebied van access management niet voldoet aan de gestelde normen voor toegangsbeveiliging, vanwege het ontbreken van een organisatorische autorisatiematrix en op basis daarvan uitgevoerde periodieke controles op de actualiteit van de autorisaties. De CPA acht het van groot belang dat de toezeggingen worden uitgevoerd die door Wigo4it op de vergadering van 26 januari 2017 zijn gedaan en dat deze werkzaamheden in 2017 gereed zijn.

De CPA ontvangt graag zo spoedig als mogelijk van u het Assurancerapport 2016 en het "in control statement" over 2016. Van Wigo4it ontvangt de CPA graag een schriftelijke bevestiging van en planning voor de gemaakte afspraken. De CPA vraagt u om te bevorderen dat deze bevestiging er komt en dat de afspraken worden opgevolgd. Voor deze afspraken verwijs ik u hier kortheidshalve naar de notulen van de vergadering over het betreffende agendapunt.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

5.1, 2, e Hoogachtend.

5.1, 2, e

De heer mr. dr. U van de Pol
Voorzitter Commissie Persoonsgegevens Amsterdam

Commissie Persoonsgegevens Amsterdam
Uittreksel van het concept-verslag van de besloten vergadering op donderdag 26 januari 2017

Aanwezigen Commissie Persoonsgegevens Amsterdam:
mevrouw mr. E. van Hasselt, mevrouw. drs. M. McCabe, de heer mr. dr. U. van de Pol (voorzitter), de heer drs. R.E.A. de Vroom,
Ambtelijk secretaris: mevrouw. mr. 5.1, 2, e

Afwezig: de heer drs. C. de Bakker, de heer mr. R.W. Henrotte

Verslag: de heer 5.1, 2, e

Bij agendapunt 8:
Wigo4it: de heren 5.1, 2, e , 5.1, 2, e (directiesecretaris) en 5.1 5.1, 2, e (adjunct-directeur); de heer 5.1 5.1, 2, e (Cluster Sociaal), de heer mr. 5.1, 5.1, 2, e (Privacy- en Informatiebeveiliging coördinator cluster Sociaal); de heer 5.1, 2, e (emeritus), met bijzondere toestemming.

8. Wigo4it

De voorzitter heet de bezoekers welkom. Zij zijn gevraagd te komen, omdat de CPA reeds lang twijfels heeft of bij Wigo4it wel alles op orde is. De CPA is al op werkbezoek geweest en de presentatie toen nam die zorgen voor een groot deel weg. Maar de audits geven aan dat niet al die toen gepresenteerde voornemens zijn gerealiseerd.

Wigo4it merkt op dat niet lang na het werkbezoek de assurance audit is verricht die nog één beperking aangaf. Dat was een verbetering ten opzichte van vorige audits die veel meer beperkingen opleverden. Voor de overheidscorporatie was dit een teken dat men op de goede weg was. Bij de ontwikkeling van het in control statement is het bedrijf op weg om daarbij minder afhankelijk te worden van externe audits en meer zelf voor te bereiden, zodat de externe partij zich kan beperken tot de validatie. Voor steeds meer beheersprocessen wordt een in control statement afgegeven. In 2015 waren dat er nog vier, in 2016 zes en voor 2017 worden dat er negen. In 2015 was er een beperking op het gebied van access management, met name in het autorisatiebeheer. De aanbevelingen voor verbetering zijn opgepakt, maar de conclusie is nu dat die te weinig hebben opgeleverd, omdat te veel is uitgaan van een top-down benadering. Daarom is men nu begonnen met een bottom-up aanpak met een maandelijks terugkerende compliance verificatie. Er wordt nu gekeken naar wat er op de werkvloer actueel speelt als basis voor de autorisatiematrix. Die koerswijziging is dit jaar ingezet. Zo ontwikkelt men iteratief steeds meer verfijnde bedrijfsregels. Een algemene bedrijfsregel is bijvoorbeeld dat er in de kantooromgeving niets aan klantgegevens kan worden gewijzigd. Stapje voor stapje wordt ontleed tot welke gegevens iemand op een bepaalde plek of rol wel toegang mag hebben en dat leidt tot autorisatie op maat. Het grootste risico is dat medewerkers ten onrechte in staat zijn klantgegevens te

manipuleren. Daarvoor worden zogenaamde Chinese muren ter afscherming in het systeem opgenomen. Daardoor wordt de groep medewerkers met toegang tot die gegevens beperkt. Maar de databasebeheerders kunnen in theorie ook bij die gegevens komen.
De vraag is hoe je dat risico kunt beperken. Een rancuneuze medewerker kan ook als de autorisatie goed geregeld is, veel schade aanrichten. Het bedrijf heeft er nooit doekjes om gewonden dat de beheersing op dit punt onvoldoende was. Maar de veiligheid betreft meer dan alleen de autorisatie. Met de nu gekozen aanpak verwacht men de zaken wel in control te krijgen.

De CPA merkt op dat het punt in 2015 was dat men dergelijk gedrag zelfs niet kon traceren en dat er op dat gebied nog steeds geen schone verklaring is. Ook nu lijkt het weer vooral te gaan om voornemens voor zaken die al lang goed geregeld hadden moeten zijn. Voor de CPA is het van belang dat de overheidscorporatie waar zo veel geld en vertrouwelijke gegevens omgaan, niet voldoet aan de privacyrichtlijnen van Amsterdam.

De voorzitter merkt op dat de afgelopen zeven jaren herhaaldelijk gewezen is op het belang van logging beleid, accessmanagement en autorisatieregels. De zorgen zijn nog steeds niet weggenomen en de vraag is of het vanuit de adviserende en toezichthoudende rol van de CPA niet tijd wordt het college te waarschuwen. Hij wil weten hoever de organisatie nu is met het op orde krijgen van die kwesties waar de CPA over dient te adviseren.

Wigo4it zegt dat het streven is de zaken in 2017 op orde te krijgen met die nieuwe aanpak die men wel moet zien als onderdeel van de opbouw van het hele systeem binnen de organisatie. Men heeft nu geen planning paraat, maar kan wel kijken of er een realistisch haalbare termijn te bepalen valt. De logging is operationeel en wordt gehandhaafd met een maandelijks scan op afwijkingen. Er zijn tot nu toe geen securitybevindingen geweest of andere incidenten op het gebied van security. Ook zijn er geen noemenswaardige datalekken gemeld, buiten het verlies van pasjes.

De voormalig voorzitter van de CPA merkt op dat bij het ontbreken van een autorisatiematrix bij logging ook geen afwijkingen aangetroffen zullen worden. De vraag is wat dan het referentiekader is.

Wigo4it zegt dat de matrix steeds verder ontwikkeld wordt en steeds beter aangeeft tot welke bestanden een medewerker toegang heeft. In ieder geval kan vastgesteld worden of een medewerker mutaties heeft aangebracht in klantgegevens waar in beginsel uitsluitend medewerkers van de clusters in de gemeenten zelf toegang toe hebben. Elke afwijking op dat punt zou worden gesignaleerd, ook zonder goede matrix. Maar het is inherent aan het werk dat meer medewerkers die gegevens kunnen raadplegen doch alleen in de productiegegevens veranderingen kunnen aanbrengen. In de nieuwe aanpak die in ontwikkeling is, wil men dat verder verfijnen. Het bleek te complex om van bovenaf de business rules te kunnen bepalen zodat iedereen binnen de organisatie de juiste autorisaties kreeg. Men heeft te maken met het expliciteren van business rules die tot dan toe min of meer impliciet waren. Het gaat om een ICT-bedrijf voor vier gemeenten met een grote verscheidenheid aan databases. Er zijn wel 54 omgevingen te onderscheiden en dat maakt

de zaken zo complex. Daarom heeft men nu gekozen voor die bottom-up aanpak om vanuit de praktijk te kijken tot welke bestanden elke medewerker toegang nodig heeft.

De heer 5.1, 2, e stelt voor dat Wigo4it samen met het cluster Sociaal een nadere brief opstelt om antwoord te geven op de vragen die de CPA gesteld heeft met daarbij ook een planning van de opbouw van de role based access zoals die nu bottom-up in ontwikkeling is. Hij denkt dat op die wijze de CPA het vertrouwen gegeven kan worden dat men eind 2017 de processen onder controle heeft. Daar kan dan ook het assurancerapport 2016 bij gevoegd worden dat medio februari gereed is waarin een in control statement zal zijn opgenomen.

De voorzitter zegt dat het goed is dat men nu in vertrouwelijkheid openlijk over de al zeven jaren slepende en diep zittende zorgen kan spreken. Er is verbazing dat het proces nog steeds in ontwikkeling is en sommige leden vragen zich af of de prioriteiten wel juist gesteld zijn in het verleden. Er gaan miljarden om in het bedrijf en men zal aan de Amsterdamse privacyregels moeten voldoen. De nieuwe aanpak kan vertrouwen wekken en een document met een strakke planning waar de CPA de organisatie dan ook strikt op kan aanspreken, zou dat vertrouwen versterken. Hij wil dat document en het assurancerapport 2016 dan wel graag uiterlijk 1 maart ontvangen. Verder lijkt het hem verstandig de communicatie nu rechtstreeks met de CPA te laten verlopen en niet zoals tot nu toe gebruikelijk via het cluster Sociaal.

De voorzitter brengt de toegankelijkheid van het gebouw ter sprake. Hij vraagt of het mogelijk is dat men als eenmaal toegelaten bezoeker achter elk scherm kan plaatsnemen. Ook is hij benieuwd of er extra afgeschermde ruimtes zijn voor de toegang tot databestanden met extra risico's.

Wigo4it geeft aan dat mede op verzoek van de G4 gekozen is voor het open kantoorconcept, zodat medewerkers elkaar en hun G4-collega's gemakkelijk kunnen ontmoeten. De directie acht dit verantwoord binnen de risico-afweging. Databestanden met extra risico's zijn allemaal elders in datacenters ondergebracht. Op de eerste verdieping zit een receptie en is een tourniquet. Achter dat tourniquet is alles open van 8.00 tot 17.00 uur. Daarna zit weer alles op slot en kan men alleen met een pasje naar binnen. In het pand zelf zijn geen data aanwezig. Daar kan men alleen bij als men heeft ingelogd, maar men kan geen data mee naar buiten nemen.

De CPA vraagt hoe het staat met het continuïteitsmanagement en hoe de data beschermd zijn tegen calamiteiten.

Wigo4it geeft aan dat de databestanden zijn ondergebracht bij twee externe datacenters die de houding verzorgen. Bij het ene datacenter is een formele third party-overeenkomst, het andere toont via maandelijkse rapportages aan dat de assurance op orde is. In de audits is dat altijd akkoord bevonden. Voor calamiteiten is een zogenaamde fill-overregeling getroffen tussen die twee datacenters.

De voorzitter constateert dat er in afwachting van de toegezegde documenten op dit moment geen vragen meer zijn. Hij verzoekt die rechtstreeks aan de ambtelijk secretaris toe te sturen en haar ook op de hoogte te houden als er kinken in de kabel komen. Hij bedankt de bezoekers voor hun komst en zegt het gesprek nuttig gevonden te hebben. Hij is blij dat de organisatie de zorgen van de CPA deelt en eraan werkt om zaken zo te krijgen als ze zouden moeten zijn.
Van de commissie zal een brief uitgaan met de gemaakte afspraken en als bijlage het verslag van deze bespreking. De brief zal ook gericht worden aan de gespreksdeelnemers, de CIO en de Stedelijk directeur Sociaal.