Cruquiusweg 5
Postbus 94652
1090 GR Amsterdam
Telefoon 5.1, 5.1, 2, e
Fax 5.1,5.1, 2, e
www.amsterdam.nl

Gemeente Amsterdam

Commissie Persoonsgegevens

Retouradres: Postbus 94652, 1090 GR Amsterdam

CIO-office
CISO
Tav 5.15.1, 2, e
Postbus 94652
1090 GR Amsterdam

Datum	3 december 2013
Ons kenmerk	U130226
Behandeld door	Mw. 5.1, 2, e
Doorkiesnummer	5.1, 2, e
Faxnummer	
E-mail	5.1, 2, e @amsterdam.nl
Bijlage	1
Onderwerp	Advies Commissie Persoonsgegevens Amsterdam

Geachte heer 5.1, 2, e ,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam van 10 oktober jl. was u aanwezig in de hoedanigheid van CISO (Chief Information Security Officer).

Het onderwerp "Incidentenregistratie en datalekken' was geagendeerd.

Het advies van de commissie was, kort samengevat, dat het belangrijkste doel van het melden van incidenten is dat bepaald kan worden welke maatregelen moeten worden getroffen en dat informatie voorhanden is hoe vaak bepaalde incidenten zich voordoen. Intern kan een voorstel gedaan worden dat op één centraal punt gemeld wordt. Een centrale registratie is van belang. Van belang is hoe de gemeente als publiekrechtelijke rechtspersoon reageert op datalekken. Verder is het een natuurlijke reactie om incidenten "onder het kleed" te vegen. De vraag is hoe dit kan worden doorbroken. Het is een verplichting, maar op welke wijze wordt duidelijk gemaakt dat het nut heeft om incidenten en datalekken te melden en dat het baat. De CISO heeft de taak om in gesprek te gaan aan de hand van rapportages, óók als er niet gemeld wordt. Dat valt dan op. Met name zal het management een rol van betekenis moeten spelen. De commissie blijft graag op de hoogte van de periodieke rapportages over incidenten en meldingen van datalekken.

Bijgaand treft u alsnog een zakelijke samenvatting aan van hetgeen op de vergadering is besproken.

Ik vertrouw er op u aldus voldoende geïnformeerd te hebben.

Met vriendelijke groet,

5.1, 2, e

.1, 2, e (ambtelijk secretaris)

Commissie Persoonsgegevens Amsterdam

Uittreksel van het verslag van de openbare vergadering op donderdag 10 oktober 2013

Openbaar deel.

10. Incidentenregistratie en wetsvoorstel datalekken

Er is geen documentatie voor het agendapunt.

De CISO bespreekt het wetsvoorstel meldplicht datalekken. Ook komt vanuit Europa nieuwe wetgeving (Europese dataprotectieverordening) die het melden van datalekken verplicht.

Niet meteen helder is wat een datalek is. Wat is de definitie van een datalek?

Er komt ook een meldplicht voor cybercrime incidenten. Er zijn dus verschillende meldplichten te onderscheiden.

De CISO adviseert en houdt toezicht op het registreren van beveiligingsincidenten. Er zijn verschillende spelers. Het CIO office maakt beleid. Als er nieuwe wetgeving komt is het logisch dat er beleid komt om de wet te implementeren. Straks komen er RVE's (Resultaatverantwoordelijke Eenheden). Dat worden er 64. Dit zijn meer organisatieonderdelen dan de gemeentelijke organisatie nu kent. De vraag is of er straks 64 contactpersonen zijn. Er komen straks ook clusters die de RVE's aansturen.

De beoogd clusterdirecteuren gaan de clusters nu inrichten. Er wordt geïnventariseerd wat op clusterniveau aan privacy- en informatiebeveiliging moet worden gedaan.

Wie kunnen een datalek melden? Dat kan allereerst een burger zijn. Er komt veel informatie van het NCSC (nationaal cybersecurity centrum). Ook komt informatie van de AIVD. Het probleem is dat alles wat de AIVD weet, geheim is. Over dit onderwerp vindt overleg plaats. Er komt ook informatie uit de diensten. Dit betreft echter niet veel informatie. Er moet aan gewerkt worden (c.q. het moet beloond worden). Er worden tot slot audits gehouden door het CIO office. Bijvoorbeeld naar websites die mogelijk lek zijn. Uit deze audits volgt informatie.

Als er wetgeving komt, is het logisch dat de noodzakelijke stappen worden ondernomen en dat rapportages gemaakt worden. Het is ook logisch als een rapportage aan de secretaris wordt geleverd. Bijvoorbeeld per kwartaal.

Gevraagd wordt of een incident wordt beschouwd als een datalek.

De CISO zegt dat als het incident persoonsgegevens betreft, het om een datalek gaat. Het is wel de vraag of een potentieel datalek als een datalek moet worden beschouwd.

De commissie zegt dat een dergelijk incident bij de procedure hoort te worden betrokken. Het is een categorie van een incident. Het categoriseren van incidenten is van belang. Ook een potentieel datalek is een incident en behoort tot de incidentenregistratie. De verantwoordelijke moet op de hoogte worden gebracht. De reden daarvoor is dat de verantwoordelijke maatregelen moet treffen. Of het incident vervolgens moet worden gemeld aan het CBP is een andere vraag. Het gaat om het leren van de incidenten en het treffen van de juiste maatregelen. De meldplicht is een stok achter de deur. Ook als melden niet verplicht is, moet de organisatie de nodige maatregelen treffen. Ook als de wet het melden nog niet verplicht stelt, is het noodzakelijk dat de organisatie doet aan het registreren en rapporteren over incidenten.