Rekenkamer
ROTTERDAM

informatiebeveiliging

mei 2016

Rekenkamer ROTTERDAM

1 inleiding

1-1 aanleiding

In februari 2016 werd de gemeente Rotterdam geconfronteerd met een datalek waarbij namen, adresgegevens en burgerservicenummers (BSN) uit belastingbestanden van de gemeente (periode 1996-2004) via het internet opvraagbaar zijn geweest. Conform de meldplicht datalekken, die per 1 januari 2016 van kracht is, heeft de gemeente Rotterdam dit lek gemeld bij de Autoriteit Persoonsgegevens. De ruim 25.000 personen wiens gegevens het betrof, heeft de gemeente per brief geïnformeerd. Daarnaast is een gespecialiseerd bureau ingeschakeld om te onderzoeken of de gegevens daadwerkelijk geraadpleegd zijn en is de gemeente op grond van het protocol Onderzoek Vermoeden Misstand en Integriteitsschending een onderzoek gestart naar de ambtenaar die de gegevens toegankelijk heeft gemaakt.

In algemene zin hebben gemeenten als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens[1] in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen.

In de onderzoeksprogrammering voor 2016 heeft de rekenkamer aangegeven in 2016 mogelijk een onderzoek te starten naar de kwaliteit van de beveiliging van (bijzondere) persoonsgegevens.[2] Naar aanleiding van het hiervoor beschreven datalek heeft de gemeenteraad op 17 maart 2016 een motie aangenomen waarin de Rekenkamer wordt verzocht direct te starten met dit onderzoek naar de informatiebeveiliging van de gemeente Rotterdam en daarin het datalek mee te nemen. De rekenkamer heeft per brief d.d. 23 maart 2016 aangegeven gehoor te geven aan dit verzoek. Deze onderzoeksopzet licht toe hoe de rekenkamer invulling geeft aan het onderzoek.

1-2 leeswijzer

Paragraaf 2 licht de beleidsmatige, juridische en organisatorische context toe. Aansluitend komt in paragraaf 3 de doel- en vraagstelling van het onderzoek aan de orde en de afbakening van het onderzoek. In paragraaf 4 wordt de onderzoeksaanpak beschreven en tot slot komt in paragraaf 5 de planning en organisatie van het onderzoek aan de orde.

1 Een persoonsgegeven is iedere vorm van informatie die direct over iemand gaat of naar deze persoon te herleiden is. Bij bijzondere persoonsgegevens gaat het om informatie over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden. Bijzondere persoonsgegevens mogen niet gebruikt worden, tenzij daarvoor een wettelijke uitzondering geldt. Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

2 Brief Rekenkamer Rotterdam, onderzoeksprogrammering 2016, 8 februari 2016 – In deze brief is het onderwerp informatiebeveiliging als reserve geagendeerd voor 2016. In principe beoogde de rekenkamer een onderzoek naar informatiebeveiliging in 2016 te starten, tenzij de raad op dit terrein zelf initiatieven richting het college zou ondernemen.

2 context

2-1 beleid en regelingen gemeente Rotterdam

In deze paragraaf wordt het informatiebeveiligingsbeleid van de gemeente Rotterdam kort toegelicht, evenals een aantal regelingen en procedures die aan dit beleid gerelateerd zijn.

concern informatiebeveiligingsbeleid

In december 2013 heeft het college het concern informatiebeveiligingsbeleid vastgesteld. Het concern informatiebeveiligingsbeleid vormt het algemene kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en moet waarborgen dat de gemeente voldoet aan relevante wet- en regelgeving.[3] Het concern informatiebeveiligingsbeleid schetst hiertoe kaders en richtlijnen voor de onderwerpen die zijn weergegeven in tabel 2-1:

tabel 2-1: onderwerpen concern informatiebeveiligingsbeleid

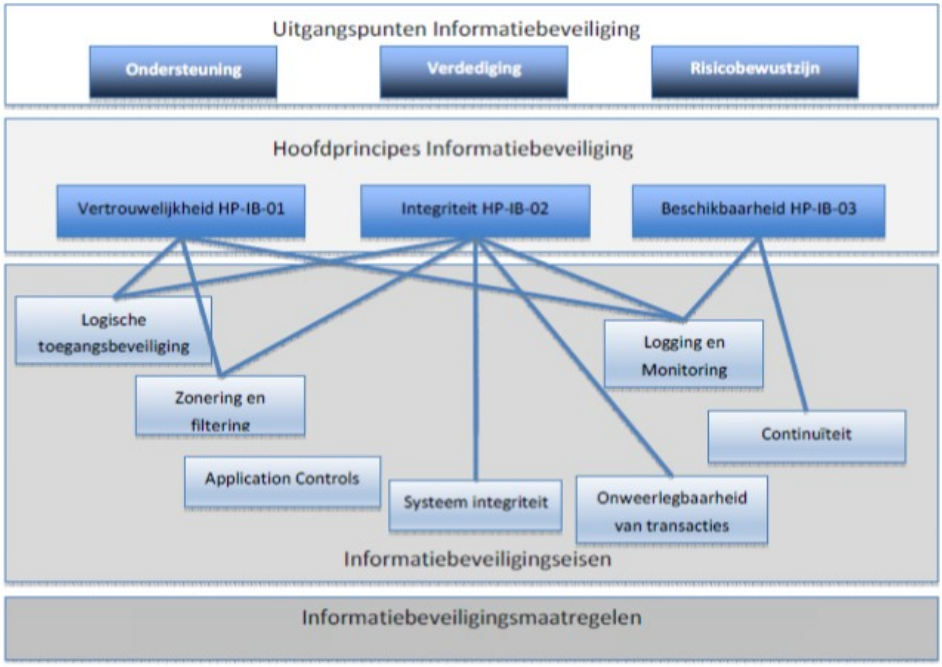
onderwerp	betreft
organisatie informatiebeveiliging	toedeling van verantwoordelijkheden, taken en rollen, inrichting PDCA-cyclus etc
gebruik van middelen en informatie	het gebruik van (privé)middelen en gemeentelijke informatie en de wijze van classificatie van gegevens
personeel	organisatorische aspecten t.a.v. het personeel en de wijze waarop bewustwording rondom het thema informatie-veiligheid geborgd moet worden
fysieke beveiliging	maatregelen om onbevoegde toegang tot gebouwen en informatie van de gemeente te voorkomen
beveiliging van apparatuur en informatie	maatregelen voor een correct en veilig gebruik van ICT-voorzieningen
logische toegangsbeveiliging	maatregelen om de toegang tot informatie te beheersen
beveiliging van informatiesystemen	maatregelen om te borgen dat beveiliging integraal deel uit maakt van informatiesystemen
beveiligingsincidenten	wijze van handelen bij beveiligingslekken of beveiligings-incidenten
bedrijfscontinuïteit	maatregelen om onderbreking van activiteiten te voorkomen en kritische informatiesystemen te beschermen tegen storingen of rampen
naleving	maatregelen om schending van wet- en regelgeving, contractuele verplichtingen en beveiligingseisen te voorkomen

concern informatiebeveiligingsarchitectuur

Het document ‘concern informatiebeveiliging – component architectuur’ geeft een praktische uitwerking van het concern informatiebeveiligingsbeleid voor de inrichting van de informatiebeveiliging. De uitgangspunten, hoofdprincipes en beheersmaatregelen die in het document zijn uitgewerkt zijn weergegeven in figuur 2-1.

3 Gemeente Rotterdam, Concern informatiebeveiligingsbeleid 2014, 10 december 2013, pagina 3.

figuur 2-1 samenhang uitgangspunten, principes en maatregelen



Bron: Gemeente Rotterdam, concern informatiebeveiliging - component architectuur, 15 december 2014.

Uitgangspunten zijn dat informatiebeveiliging de risico's van het werken met gevoelige informatie beoogt te beheersen (ondersteuning), de organisatie beschermt wordt tegen beveiligingsincidenten (verdediging) en het risicobewustzijn binnen de organisatie wordt vergroot (risicobewustzijn). Hiertoe gelden de volgende hoofdprincipes voor informatiebeveiliging:

- vertrouwelijkheid: de data-eigenaar verschaft alleen geautoriseerde gebruikers toegang tot vertrouwelijke gegevens;
- integriteit: de dataverantwoordelijke waarborgt de integriteit (juistheid, volledigheid en tijdigheid) van gegevens;
- beschikbaarheid: de beschikbaarheid van informatie en IT voldoet aan de gemaakte continuïteitsafspraken.

regeling ICT en informatiegebruik

Vanaf april 2012 is binnen de gemeente Rotterdam de regeling ICT en informatie-gebruik van kracht. Hierin zijn de regels voor het gebruik van gemeentelijke ICT-middelen en gemeentelijke informatie vastgelegd en regels voor het monitoren van dit gebruik. De regeling geldt voor alle medewerkers van de gemeente Rotterdam en geldt zowel bij gebruik van gemeentelijke ICT-middelen als bij gebruik van privé middelen. In de regeling is onder meer bepaald dat medewerkers alleen toegang hebben tot gegevens waarvoor ze zijn geautoriseerd en medewerkers maatregelen moeten treffen tegen verlies of verkeerd gebruik van gegevens.

procedure aanvraag externe dataverbindingen

Deze procedure betreft het toekennen van toegang tot het Rotterdamse netwerk aan externe partijen. De procedure beschrijft de uitgangspunten die daarbij gelden, de

aanvraagprocedure die moet worden doorlopen en het toetsingskader dat daarbij geldt. De aanvragen worden getoetst door security managers van het cluster BCO.

protocol meldplicht datalekken
Per 1 januari 2016 geldt op grond van de Wet bescherming persoonsgegevens de verplichting om geconstateerde datalekken waarbij sprake is van (mogelijk) ernstige gevolgen voor de privacy te melden bij de Autoriteit Persoonsgegevens. Het protocol meldplicht datalekken beschrijft hoe de gemeente Rotterdam omgaat met dergelijke datalekken. Hiertoe bevat het protocol afwegingskaders voor het geval sprake is van en vermoeden van een datalek en het te doorlopen proces in geval van een melding.

2-2 meerjarenplan concern informatiebeveiliging

In maart 2015 heeft de concerndirectie het meerjarenplan concern informatie-beveiliging ontwikkelpad 2015-2017 vastgesteld.[4] In het meerjarenplan wordt geconstateerd dat de organisatorische aspecten van informatiebeveiliging onderbelicht zijn en bij de meeste clusters niet of nauwelijks zijn ingevuld, met het gevolg dat taken rondom risicobewustwording, sturing op naleving en control blijven liggen. Technische verbeteringen zijn volgens het meerjarenplan nog veelal ad hoc en vooral gericht op bescherming van buiten af. Tot slot wordt opgemerkt dat de beveiligingsfunctie afhankelijk is van enkele personen, wat de functie kwetsbaar maakt.[5]

Doel van het meerjarenplan is de realisatie van een juist gepositioneerde en gedimensioneerde informatiebeveiligingsfunctie.[6] Hiertoe zijn op vier sporen de volgende ambities geformuleerd:

1 beleid: het Rotterdamse beleid is in lijn met landelijke en Europese wet- en regelgeving voor informatiebeveiliging en privacybescherming en afgestemd op gemeentelijke risico's.
2 inrichting informatiebeveiliging: informatiebeveiliging is als integrale taak en verantwoordelijkheid ingericht, waarbij de rollen evenredig tussen alle verantwoordelijken zijn verdeeld.
3 control: informatiebeveiliging is ingebed in het primaire proces en onderdeel van concern risicomanagement. Hierover wordt op professionele wijze verantwoording afgelegd.
4 techniek: informatiebeveiliging is ingericht conform good practices en daarover wordt op professionele wijze verantwoording afgelegd.

2-3 juridische context

Wet bescherming persoonsgegevens
De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens.[7] In artikel 13 Wbp is bepaald dat sprake moet zijn van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Er moet

4 Dit meerjarenplan is een actualisatie van het eerste meerjarenplan concern informatiebeveiliging dat in maart 2014 is vastgesteld.

5 Gemeente Rotterdam, Meerjarenplan concern informatiebeveiliging ontwikkelpad 2015-2017, 2 maart 2015, pagina 3.

6 Gemeente Rotterdam, Meerjarenplan concern informatiebeveiliging ontwikkelpad 2015-2017, 2 maart 2015, pagina 5.

7 Recent is op Europees niveau overeenstemming bereikt over de algemene verordening inzake gegevensbescherming. Deze verordening moet o.a. leiden tot een betere bescherming van gegevens van burgers. De verordening zal in 2018, na een overgangsperiode van twee jaar, van kracht worden.

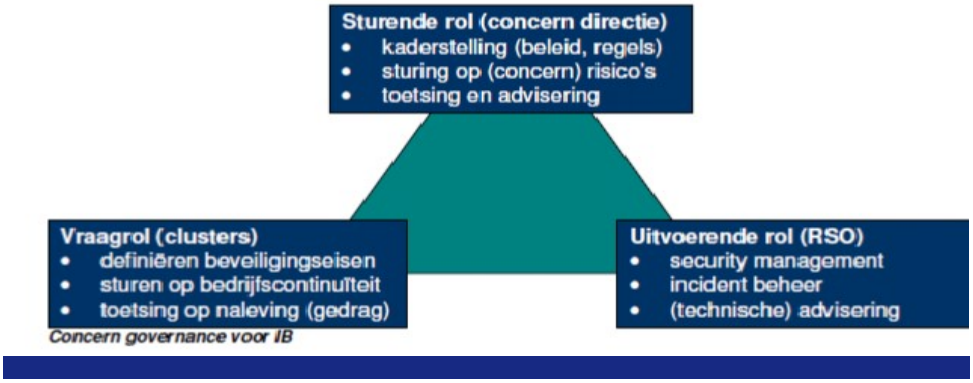
sprake zijn van een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Wet basisregistratie personen
Op de verwerking van persoonsgegevens die zijn opgenomen in de basisregistratie personen (BRP) is de Wet bescherming persoonsgegevens niet van toepassing. Het gebruik, de bescherming en beveiliging van persoonsgegevens uit de BRP is geregeld binnen het kader van de Wet basisregistratie personen (Wet BRP). In artikel 1.11 van de Wet BRP is bepaald dat het college van B&W er zorg voor moet dragen dat de gemeentelijke voorziening rond de basisregistratie personen functioneert overeenkomstig de regels voor de technische en administratieve inrichting en werking, en de regels voor de beveiliging van de basisregistratie. De maatregelen die de gemeente Rotterdam treft ter beveiliging van de gegevens in de basisregistratie zijn vastgelegd in de beheerregeling gemeentelijke basisregistratie personen Rotterdam.

2-4 organisatorische context

Het college van B&W draagt de integrale verantwoordelijkheid voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Binnen de ambtelijke organisatie zijn de verantwoordelijkheden voor informatiebeveiliging verdeeld zoals weergegeven in figuur 2-1.[8]

figuur 2-2 concern governance informatiebeveiliging



Bron: Gemeente Rotterdam, Concern informatiebeveiligingsbeleid 2014.

3 doel- en vraagstelling

3-1 doelstelling

De rekenkamer beoogt met dit onderzoek na te gaan of de gemeente adequaat opvolging heeft gegeven aan het datalek in februari 2016 en in bredere zin na te gaan of (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Rotterdam in veilige handen zijn.

3-2 vraagstelling

De centrale onderzoeksvraag luidt als volgt:
Heeft de gemeente Rotterdam adequaat opvolging gegeven aan het datalek in februari 2016 en zijn (bijzondere)persoonsgegevens en andere gevoelige informatie bij de gemeente Rotterdam in veilige handen?

8 Per 2016 is het cluster RSO omgevormd naar het cluster BCO.

De centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen:

1 Welke maatregelen heeft de gemeente Rotterdam genomen na het datalek in februari 2016 en zijn deze voldoende om dergelijke incidenten in de toekomst redelijkerwijs te voorkomen?
2 Heeft de gemeente Rotterdam in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?
3 Heeft de gemeente Rotterdam voldoende maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?
4 Is het mogelijk oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Rotterdam in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?

3-3 afbakening

Met betrekking tot de afbakening van dit onderzoek zijn de volgende punten relevant:

- In het kader van deelvraag 1 zal de rekenkamer gebruik maken van de resultaten van de onderzoeken die in opdracht van de gemeente zijn uitgevoerd naar het datalek.
- In het kader van deelvraag 2 beoogt de rekenkamer na te gaan of de gemeente de belangrijkste risico's (met in potentie de grootste impact) in beeld heeft. De rekenkamer zal dus niet beoordelen of de gemeente *alle* potentiële risico's in beeld heeft. Als blijkt dat de gemeente de belangrijkste risico's niet of onvoldoende in beeld heeft zal de rekenkamer de belangrijkste risico's zelf in kaart brengen.
- In het kader van deelvraag 3 kijkt de rekenkamer zowel naar maatregelen die op niveau van het concern worden getroffen, als maatregelen binnen de individuele clusters. Daarbij neemt de rekenkamer zowel technische als organisatorische (o.a. gericht op de beheersing van het gedrag van medewerkers) beveiligingsmaatregelen in ogenschouw.
- In het kader van deelvraag 4 zal de rekenkamer testen of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens in systemen van de gemeente Rotterdam en tot andere gevoelige informatie die de gemeente in beheer heeft, zoals bijvoorbeeld financiële of commercieel gevoelige informatie.

4 onderzoeksaanpak

4-1 documentstudie en interviews

In het kader van dit onderzoek zal de rekenkamer o.a. de volgende documenten bestuderen:

- onderzoeksrapporten en evaluaties m.b.t. het datalek;
- overige documenten m.b.t. de opvolging van het datalek;
- beleidsstukken, regelingen, procedures e.d. ten aanzien van de informatiebeveiliging en het beheer van (bijzondere)persoonsgegevens;
- meerjarenplan concern informatiebeveiliging;
- voortgangs- en auditrapportages m.b.t. informatiebeveiliging en het beheer van (bijzondere)persoonsgegevens;
- risico- en/of dreigingsanalyses;
- documenten m.b.t. informatiebeveiliging en het beheer van (bijzondere) persoonsgegevens bij de gemeentelijke clusters.

In het kader van dit onderzoek zullen interviews worden gehouden met:
- de wethouder organisatie;
- ambtenaren van het cluster BCO die verantwoordelijk zijn voor informatiebeveiliging of taken uitvoeren op dit gebied;
- ambtenaren van de overige clusters die zich bezighouden met informatiebeveiliging en/of het beheer van (bijzondere)persoonsgegevens.

4-2 testen mogelijkheden oneigenlijke toegang

De rekenkamer zal voor de uitvoering van dit onderzoek externe deskundigheid inhuren van een bedrijf met expertise op het gebied van informatiebeveiliging en bescherming van (bijzondere)persoonsgegevens en de specifieke kennis heeft die nodig is om te testen of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens die de gemeente in beheer heeft.

De onderzoekswerkzaamheden die voor de beantwoording van deelvraag 4 worden uitgevoerd, zullen in overleg met de externe deskundige worden bepaald. De daadwerkelijke uitvoering gebeurt in afstemming met de gemeentelijke organisatie. De rekenkamer zal voor dit deel van het onderzoek geen onderzoekswerkzaamheden uitvoeren zonder medeweten van het concern.

4-3 normenkader

In tabel 4-1 is het globale normenkader opgenomen dat de rekenkamer in dit onderzoek zal hanteren voor de deelvragen 1 t/m 3. Gezien de aard van deelvraag 4 worden bij die onderzoeksvraag geen normen gehanteerd. Het normenkader zal in overleg met de externe deskundigen die voor dit onderzoek worden ingehuurd, nader worden gespecificeerd.

tabel 4-1: normenkader

deelvraag	normen
1. Welke maatregelen heeft de gemeente Rotterdam genomen na het datalek in februari 2016 en zijn deze voldoende om dergelijke incidenten in de toekomst redelijkerwijs te voorkomen?	• De gemeente heeft de oorzaken en gevolgen van het datalek in februari 2016 afdoende onderzocht. • Op basis van de onderzoeksbevindingen heeft de gemeente maatregelen getroffen die een dergelijk datalek in de toekomst redelijkerwijs kunnen voorkomen.
2. Heeft de gemeente Rotterdam in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?	• Op concernniveau en binnen de individuele clusters worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt. • In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd. • De risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens.
3. Heeft de gemeente Rotterdam voldoende maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?	• De gemeente heeft technische maatregelen getroffen die de risico's doen afnemen. • De gemeente heeft organisatorische maatregelen getroffen die de risico's doen afnemen.

- Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoons-gegevens die de gemeente in beheer heeft.

5 organisatie en planning

5-1 organisatie

Dit onderzoek zal worden uitgevoerd door een onderzoeksteam van de rekenkamer dat gezien de aard van het onderzoek wordt aangevuld met externe deskundigen. Het team van de rekenkamer bestaat uit:

- Rolf Willemse (projectleider);
- Nicole Kuijpers;
- Rosa Ridderhof.

5-2 planning

De uitvoering van het onderzoek start in mei 2016. Publicatie van het rapport is voorzien in het najaar van 2016.