Datalekken

Uitgangspunten & protocol inzake omgang en bestrijding datalekken

rentree. thuis in Deventer

Vastgesteld MT d.d. 15 december 2016

Documentgegevens

Documentinhoud:	Uitgangspunten & protocol inzake omgang en bestrijding datalekken
Ten behoeve van:	Rentree, intern
Auteur:	Henry Koster
Documentversie:	1.0

Versiehistorie

Versienummer	Datum	Status	Omschrijving wijziging
0.1	24-11-2016	Basisversie	-
0.2	28-11-2016	Review versie	Eerste versie t.b.v. interne review
1.0	07-12-2016	Definitief	Opmaak / lay-out aangepast, inhoudelijke aanvullingen & tekstuele wijzigingen doorgevoerd o.b.v. interne review

Inhoud

1 Achtergrond, aanleiding & inleiding

Per 1 januari 2016 is de Meldplicht Datalekken als onderdeel van de Wet bescherming persoonsgegevens (Wbp) van kracht. Deze aanvulling op de Wbp levert een aantal actiepunten en verplichtingen op voor gegevensverwerkende organisaties.

1.1 Meldplicht

Wat houdt deze meldplicht in? De Autoriteit Persoonsgegevens schrijft hierover: 'Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de AP zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt) [1].

Als basisregel geldt dat de meldplicht van toepassing is als door de organisatie persoonsgegevens worden verwerkt in Nederland. Onder het verwerken van persoonsgegevens verstaan we elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. De meldplicht geldt daarbij als je verantwoordelijk bent voor de verwerking. Dat ben je als je het doel van de verwerking en/of de middelen ervoor hebt bepaald.

Voor corporaties geldt dat:

De beoordeling van een datalek en de melding aan de AP dient zo snel mogelijk, maar binnen 72 uur plaats te vinden na het optreden van het incident. Bij het niet nakomen van de wettelijke verplichtingen is de AP bevoegd bindende aanwijzingen op te leggen of boetes tot een maximum van € 820.000 (2016, jaarlijkse indexatie mogelijk).

1.2 Wat is een datalek?

Bij een datalek denken we vaak aan het ongewenst openbaar worden van vertrouwelijke gegevens. Maar de wet hanteert een veel bredere definitie. Wettelijk ben je verplicht om 'verlies of onrechtmatige verwerking' van persoonsgegevens te voorkomen met passende technische en organisatorische maatregelen.

Een datalek is dus een incident waarbij de bescherming van persoonsgegevens is doorbroken en waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Dat kan van alles zijn: van het 'op straat belanden' tot het per ongeluk verwijderen van een belangrijk overzicht met persoonsgegevens, zonder dat er een reservekopie van het bestand is.

[1] De samenvatting van het wettelijk beleidskader is toegevoegd als bijlage in dit document.

Of het betreffende datalek ook daadwerkelijk aan de autoriteit persoonsgegevens (AP) en de betrokkenen gemeld moet worden, hangt af van diverse factoren en zal situationeel beoordeeld dienen te worden. De belangrijkste afweging is of er ernstige nadelige gevolgen voor de betrokkenen te verwachten zijn[2] .

In het kort komt de afweging op het volgende neer:

2 Er is een verschil tussen een datalek en een beveiligingslek. Het verschil is belangrijk omdat een beveiligingslek niet verplicht gemeld hoeft te worden, terwijl het melden van een datalek wel verplicht is.

We spreken van een datalek als er sprake is van toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie. Voorbeelden hiervan zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. Er is een toename aan criminaliteit binnen het stelen van informatie, omdat dit veel oplevert. Maar een datalek kan ook al ontstaan door gevoelige informatie naar de verkeerde persoon te e-mailen of door de naïviteit van onszelf door bijvoorbeeld te makkelijke wachtwoorden te gebruiken. Dit zijn allemaal voorbeelden van datalekken. Maar, als er alleen sprake is van een zwakke plek in de beveiliging, dan spreken we van een beveiligingslek en niet van een datalek. Een beveiligingslek hoeft dus niet verplicht gemeld te worden.

2 Stand van zaken

2.1 Doelstelling

Rentree wil voldoen aan de (nieuwe) meldplicht datalekken die, als aanvulling op de wet bescherming persoonsgegevens (Wbp), per 1 januari 2016 in werking is getreden.

Daarvoor worden in operationele zin de "Beleidsregels voor toepassing van artikel 34a van de Wbp inzake De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) d.d. 8 december 2015" gevolgd. Dit document is separaat beschikbaar en dient als detailhandleiding voor de omgang met de wet meldplicht datalekken. Als zodanig onlosmakelijk verbonden aan de inhoud van dit document. Hiertoe is tevens een plan van aanpak opgesteld en uitgevoerd (conform fasering zoals in
plan van aanpak 20151212_PvA_Meldingplicht_datalekken.doc, versie 1.0 vermeld).

2.2 Stand van zaken

I.v.m. het vertrek van de trekker en de overdracht naar een nieuwe collega is de planning in inhoudelijk bereik niet conform beoogd tijdsbestek en originele planning gerealiseerd. Onderliggend document geeft de actuele status, overwegingen en keuzes weer en bevat als resultaat het protocol "Datalekken Rentree".

2.2.1 Stand van zaken conform de faseringen uit het plan van aanpak

Fase	Omschrijving	Resultaat	Voorstel vervolg
0	Voorbereiding	Afgerond	n.v.t.
1	Opstart	Afgerond	n.v.t.
2	Informatiestromen in kaart	Uitgevoerd	Applicaties op hoofdlijnen in beeld gebracht t.b.v. bewerkersovereenkomsten om te voldoen aan wetgeving.
3	Risicoanalyse	Op hoofdlijnen uitgevoerd	Geen detailuitwerking. Omgang met persoonsgegevens in algemene zin borgen. Detailanalyse niet noodzakelijk voor voldoen aan wetgeving. Elk incident zal situationeel beoordeeld worden conform het protocol "Datalekken Rentree"
4	Stel een meldingsprotocol op	Uitgevoerd, inclusief eigen model bewerkersovereenkomst Rentree	Communicatie in organisatie
5	Informeer medewerkers	Deels uitgevoerd	Communicatie in organisatie december 2016 & januari 2017 middels personeelsbijeenkomst, organisatieoverleg & mail / ViewPoint-berichten
6	Maak afspraken met bewerkers	Deels uitgevoerd	Uiterlijk februari 2017 ontvangen van leveranciers uit 4.1 Bijlage: Bewerkersovereenkomsten

In eerste instantie zijn er werkzaamheden uitgevoerd in de fasen 0, 1 en 2 en op hoofdlijnen met betrekking tot fase 3. M.b.t. fase 5 is er een kickoff-sessie geweest ten behoeve van

bewustwording bij een aantal medewerkers van Rentree (tevens bedoeld om informatie te verzamelen).

Met een aantal leveranciers is in 2016 reeds een bewerkersovereenkomst afgesloten als aanvulling op de bestaande dienstverleningscontracten en/of afspraken om de wederzijdse verantwoordelijkheden en verplichtingen te borgen (fase 6). De eerste aandacht is hierbij uitgegaan naar de leveranciers van primaire systemen.

2.2.2 Voorstel

In het kader van de wetgeving & verplichtingen, wordt voorgesteld een aantal fasen nu versneld uit te voeren en af te ronden met als belangrijkste resultaat het protocol “Datalekken Rentree”, een model bewerkersovereenkomst Rentree en communicatie / presentaties met uitleg t.b.v. bewustwording.

Er is afgezien van een uitgebreide en volledige informatie- en risico-analyse per veld of systeem. Deze is later mogelijk als het overkoepelend informatiebeveiligingsbeleid opgesteld gaat worden en waar gegevensbescherming in brede zin van de definitie een onderwerp is.

Motivatie voor deze keuzes:

- De initiële planning (zoals geformuleerd in het plan van aanpak) is niet gehaald, maar de relevantie om te voldoen aan de wetgeving is gebleven;
- De wet meldplicht datalekken en privacy wetgeving zijn generiek toepasbaar en focussen op de persoonsgegevens. De analyse welke gegevens waar staan en welke expliciete risico’s er per applicatie bestaan, zijn maatwerk, later invulbaar en vanwege de inhoudelijke situationele beoordeling per incident daarin ondervangen.
- De bewerkersovereenkomsten zijn niet universeel (toepasbaar) per leverancier, maar verwijzen wel allemaal naar de wettelijke kaders. Daardoor zijn deze niet afhankelijk zijn van de informatie- en risicoanalyses per applicatie / informatiesysteem;
- In eerste instantie willen we voldoen aan het wettelijk kaders en bewustwording bij medewerkers / onderaannemers / bewerkers. Dit omdat de technische maatregelen geborgd zijn door de leveranciers van primaire systemen middels ISO27001-verklaringen en toelichtingen[3] (en qua verantwoordelijkheden ingevuld gaan worden door bewerkersovereenkomsten), de wetgeving reeds operationeel is en bewustwording bij de factor mens de grootste bijdrage levert aan het beheersen van data- en informatielekken.

2.3 Besluitvorming & vervolg

Voor nu wordt kennisname en besluitvorming gevraagd op 3 onderdelen:

- Protocol Datalekken Rentree
- Model bewerkersovereenkomst Rentree
- Uitgangspunten communicatie & bewustwording omtrent Datalekken

2.3.1 Protocol Datalekken Rentree

Werkwijze en afhandeling van incidenten die als datalek zijn geclassificeerd vast te stellen. Dit protocol is opgenomen in hoofdstuk 3 Protocol Datalekken Rentree.

2.3.2 Model bewerkersovereenkomst Rentree

Met alle partners en bewerkers van data van Rentree (waarbij Rentree als opdrachtgever geldt) worden bewerkersovereenkomsten afgesloten. Zie 4.1 Bijlage: Bewerkersovereenkomsten

[3] ISO 27001 is een ISO standaard voor informatiebeveiliging -> https://nl.wikipedia.org/wiki/ISO/IEC_27001

voor een actueel overzicht.

In het geval een van de samenwerkende partners of leveranciers van informatiesystemen en/of diensten niet zelf actief voorziet in een bewerkersovereenkomst (als aanvulling op de afgesloten contracten, naar aanleiding van de wet meldplicht datalekken per 01-01-2016), is een model bewerkersovereenkomst vanuit Rentree als opdrachtgever opgesteld. Deze is bekend onder de titel: “Bewerkersovereenkomst – Rentree”. Dit document is als basissjabloon separaat beschikbaar en als zodanig verbonden met de inhoud van dit document. De laatste sjabloonversie is 1.3[4].

2.3.3 Uitgangspunten communicatie & bewustwording omtrent Datalekken

Algemene operationele uitgangspunten in de communicatie & bewustwording:

- Met samenwerkende partners die inzicht hebben in gegevens of gegevens verwerken/bewerken is een bewerkersovereenkomst aanwezig;
- Data is binnen Rentree niet openbaar toegankelijk voor derden (dat betekent dat schermen gelocked moeten worden als je de werkplek verlaat, bewust omgegaan wordt met fysieke afdrukken, USB-sticks niet of beperkt gebruikt worden)
- Toegang tot data beperkt is op basis van rechten en rollen, toegang tot USB-poorten beperkt is
- Datasets worden niet als leesbare sets / tekst via mail verstuurd
- Datasets worden niet onbeveiligd verstuurd (minimaal een wachtwoord, wat via ander medium wordt doorgestuurd, bijvoorbeeld telefoon/sms/whatsapp)
- Wachtwoorden die gebruikt worden zijn gelijk aan voorschriften van NEH-protocol / KA-omgeving (minimaal 8 karakters, 1 bijzonder karakter en minimaal 1 hoofdletter en minimaal 1 normale letter)
- Voor wat betreft de beveiliging van de digitale basisinfrastructuur wordt geleund op de maatregelen die (ISO27001-gecertificeerde) partners hebben getroffen. Hiermee worden bewerkersovereenkomsten afgesloten.
- Elk beveiligingsincident en/of datalek wordt geregistreerd[5] en conform protocol Datalekken Rentree afgehandeld. Eerste aanspreekpunt is de teamleider ICT (in de rol van operationeel beveiligingsverantwoordelijke), eerste inhoudelijke achtervang is een van de informatie-adviseurs. Escalatie vindt plaats via directeur-bestuurder (in de rol van eindverantwoordelijke informatiebeveiliging).

---

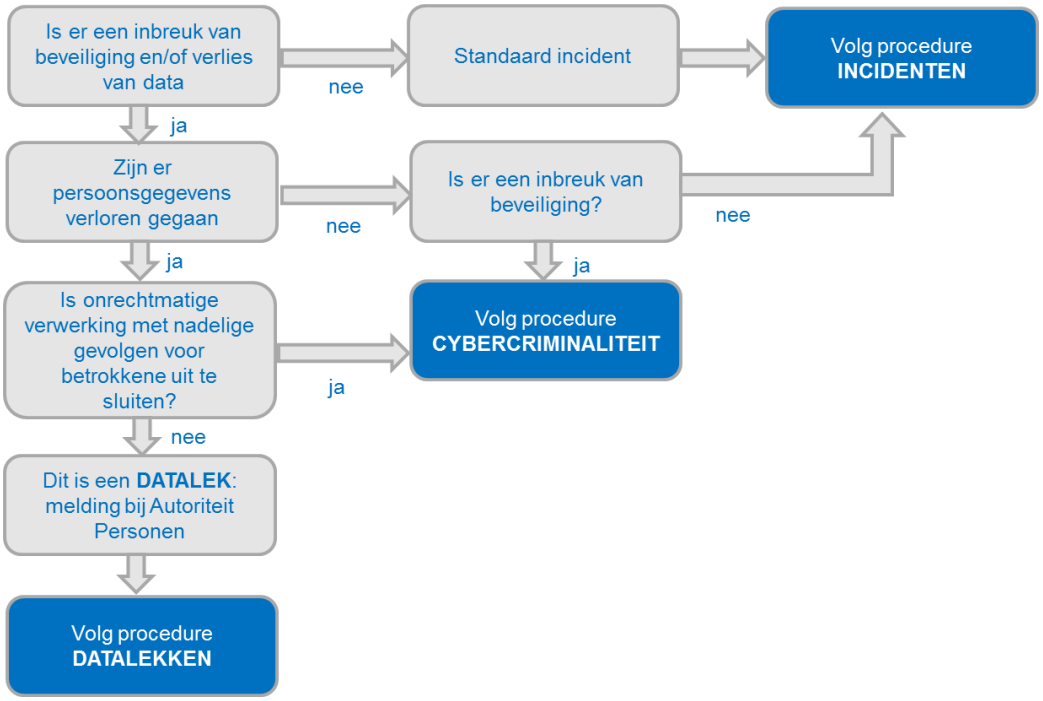
4 De modelovereenkomst is tevens verstrekt aan Enserve om her te gebruiken als basis voor bewerkersovereenkomsten met haar klanten (Woonkeus / Stedendriehoek).

5 **Documentatieplicht:** Datalekken die leiden tot een aanzienlijke kans op ernstige nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene (dat wil zeggen: alle incidenten die gemeld zijn of gemeld hadden moeten worden) moeten gedocumenteerd worden in een register (artikel 34a lid 8 Wbp). Deze bescheiden moeten minimaal een jaar worden bewaard en drie jaar wanneer wordt besloten om de betrokkene niet te informeren omdat de technische beschermingsmaatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten (artikel 34a lid 6 Wbp) of wanneer dit niet gebeurt om zwaarwegende redenen.

3 Protocol Datalekken Rentree

3.1 Afweging vooraf

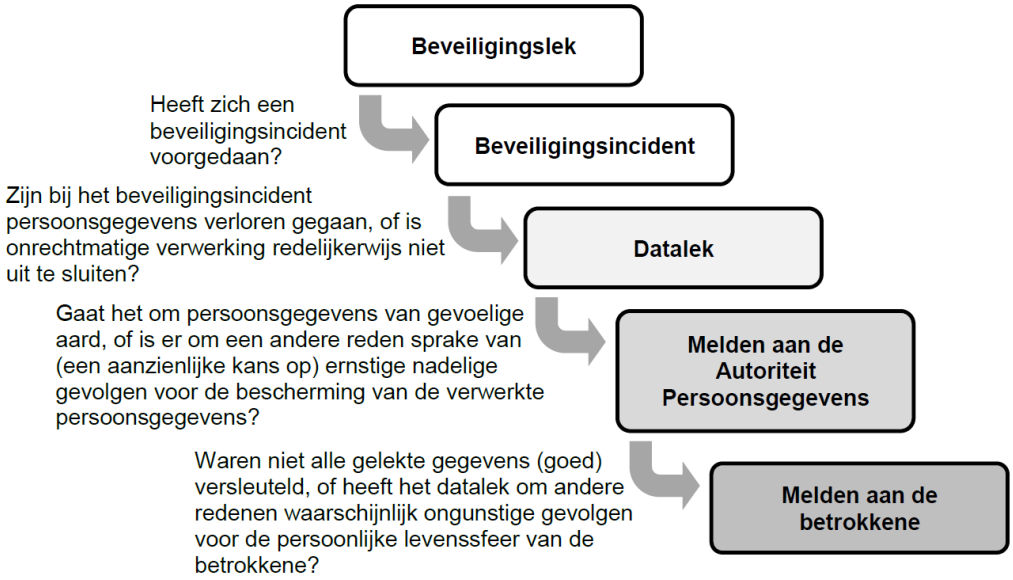
Voorafgaand aan de afhandeling van een datalek, is een afweging gedaan over de te volgen procedure (regulier incident, beveiligingsincident / cybercriminaliteit en datalekken).



3.2 Er is een incident geconstateerd met de classificatie Datalek

3.2.1 Wanneer melden en aan wie?

Verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.' Daarvoor worden in operationele zin de Beleidsregels voor toepassing van artikel 34a van de Wbp inzake De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) d.d. 8 december 2015 gevolgd. Deze geven het volgende schema weer:



3.2.2 Legenda:

- Betrokkene: degene wiens gegevens het betreft (huurder, burger, medewerker, bedrijf)
- Bewerker: partners en/of onderaannemers, welke in opdracht van Rentree toegang heeft tot gegevens of deze ver- / bewerkt
- Verantwoordelijke: Rentree. Binnen Rentree is het eerste aanspreekpunt de teamleider ICT (in de rol van operationeel beveiligingsverantwoordelijke). Deze coördineert eventuele acties & communicatie. Eerste inhoudelijke achtervang is een van de informatie-adviseurs. Escalatie vindt plaats via directeur-bestuurder (in de rol van eindverantwoordelijke informatiebeveiliging).

3.2.3 Checklist

Actie	Toelichting / omschrijving	Resultaat / kenmerk Terug te vinden in:	Datum	Tijdstip (24h)	Check √ / n.v.t
Analyse Datalek	• Een omschrijving van de aard van de inbreuk (classificatie als beveiligingsincident, prioriteit hoog) na constatering van een datalek ○ Is directe toegangsblokkering nodig, in welke mate en voor welke toegangspaden? Eventuele toegangsblokkering doorgevoerd? • De instanties waar meer informatie over de inbreuk kan worden verkregen (vanuit perspectief bewerker en/of verantwoordelijke) • de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken & de eventueel genomen nood / spoedmaatregelen • de eventueel genomen nood / spoedmaatregelen door bewerker of Rentree • een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens • de maatregelen die Rentree treft (i.s.m. een eventuele bewerker) • voorstellen tot maatregelen om de gevolgen te verhelpen	Datum tijdstip van de inbreuk en eventueel getroffen maatregelen			
Informeren AP	Rentree (als verantwoordelijke) stelt de AP onverwijld in kennis van een inbreuk op de beveiliging en levert de volgende informatie aan: • een omschrijving van de aard van de inbreuk • de instanties of contactpersonen waar meer informatie over de inbreuk kan worden	Binnen 72 uur melding bij AP, via webformulier: https://autoriteitpersoonsgegevens.nl/			

Actie	Toelichting / omschrijving	Resultaat / kenmerk Terug te vinden in:	Datum	Tijdstip (24h)	Check √ / n.v.t
	verkregen • de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken • een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens • de maatregelen die Rentree heeft getroffen • de maatregelen die Rentree voorstelt te treffen om de gevolgen te verhelpen				
Informeren betrokkene	Rentree stelt de betrokkene onverwijld in kennis van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. • Een omschrijving van de aard van de inbreuk • de instanties waar meer informatie over de inbreuk kan worden verkregen • de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken Bovenstaande is niet van toepassing indien Rentree of bewerkers passende technische beschermingsmaatregelen hebben genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens	Een persoonlijk bericht, een bericht op een website of een advertentie in de krant. Het is in ieder geval belangrijk om bij (grootschalige) datalekken zelf contact op te nemen met de pers en ze te informeren over wat er is gebeurd.			
Mitigerende maatregelen ter preventie & herstel	Afhankelijk van de situatie van datalekken / digitale lekken: hacking, ddos, datadragers of anderszins worden mitigerende maatregelen geformuleerd. Deze zijn situationeel te bepalen, waarbij leidend zijn in de afwegingen: • de bescherming van persoonsgegevens,				

Actie	Toelichting / omschrijving	Resultaat / kenmerk Terug te vinden in:	Datum	Tijdstip (24h)	Check √ / n.v.t
	• integriteit van de data, • de werking van de technische infrastructuur				
Rapportage	Rapportage van bevindingen met een toelichting intern binnen Rentree en aan directeur – bestuurder.	Registratie in primair DMS (i.c. ViewPoint) als beveiligingsincident met classificatie Datalek			
Aanvullende acties	Te definiëren per situatie, o.b.v. afspraken / terugkoppelingsmomenten, acties met betrokken partijen (klant, AP, betrokken individuen, interne afdelingen, derden)				

4 Bijlagen

4.1 Bijlage: Bewerkersovereenkomsten

In het geval een van de samenwerkende partners of leveranciers van informatiesystemen en/of diensten niet zelf actief voorziet in een bewerkersovereenkomst (als aanvulling op de afgesloten contracten, nav de wet meldplicht datalekken per 01-01-2016), is een model bewerkersovereenkomst vanuit Rentree als opdrachtgever opgesteld. Deze is bekend onder de titel: “Bewerkersovereenkomst – Rentree”. Dit document is als basissjabloon separaat beschikbaar. De laatste sjabloonversie is 1.3.

Het volgende overzicht is beschikbaar voor bewerkersovereenkomsten met leveranciers van informatiesystemen en dienstverleningsovereenkomsten.

Bewerker	Rol / applicatie	Status bewerkersovereenkomst	Datum
Wolters	Aannemer, onderhoud	Ontvangen & akkoord	17-3-2017
Salverda	Aannemer, onderhoud	Onvangen en akkoord	23-5-2017
Steenbruggen	Installatiewerk	Onderhanden	
Enserve	Woonkeus	Ontvangen & akkoord	13-3-2017
Itris	ViewPoint	Ontvangen & akkoord	15-11-2016
NEH	Hosting & infrastructuur	Ontvangen & akkoord	12-7-2016
Kroese Wevers	Loket.nl	Ontvangen & akkoord	28-2-2017
Emotion	Mailplus	Onderhanden	
Itraction	Coda financials	Ontvangen & akkoord	30-9-2016
Goudappel Coffeng	Klanttevredenheidsonderzoek	Ontvangen & akkoord	15-11-2016
VSD	Verzuimexpert	Inhoudelijk akkoord	15-02-2018
UWV	UWV Digitaal melden	N.v.t.	**
Pranger	Pranger	Ontvangen & akkoord	20-2-2017
BZT	BZT	N.v.t.	**
VIS-2	Vangnet informatie systeem	N.v.t.	**
DataB	Verwerking analoge post	Ontvangen & akkoord	15-12-2017
Coencad	Tekenwerk, opdracht TEC	Ontvangen & akkoord	12-1-2018
Slim Energiebeheer	Energieopnames, dossieronderzoek	Onderhanden	
Wocozon	Energieopnames, levering zonnepanelen	Inhoudelijk akkoord	26-3-2018

Update d.d. 8 juni 2018

** Geen opdrachtgever / opdrachtnemersrol. In de zin van bewerker, geen formele relatie -> dus geen bewerkersovereenkomst mogelijk.

4.2 Bijlage: Samenvatting wettelijk kader

Deze samenvatting is integraal overgenomen uit: “Beleidsregels voor toepassing van artikel 34a van de Wbp inzake De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) d.d. 8 december 2015”. Deze is als achtergrondinformatie opgenomen in deze bijlage.

Samenvatting

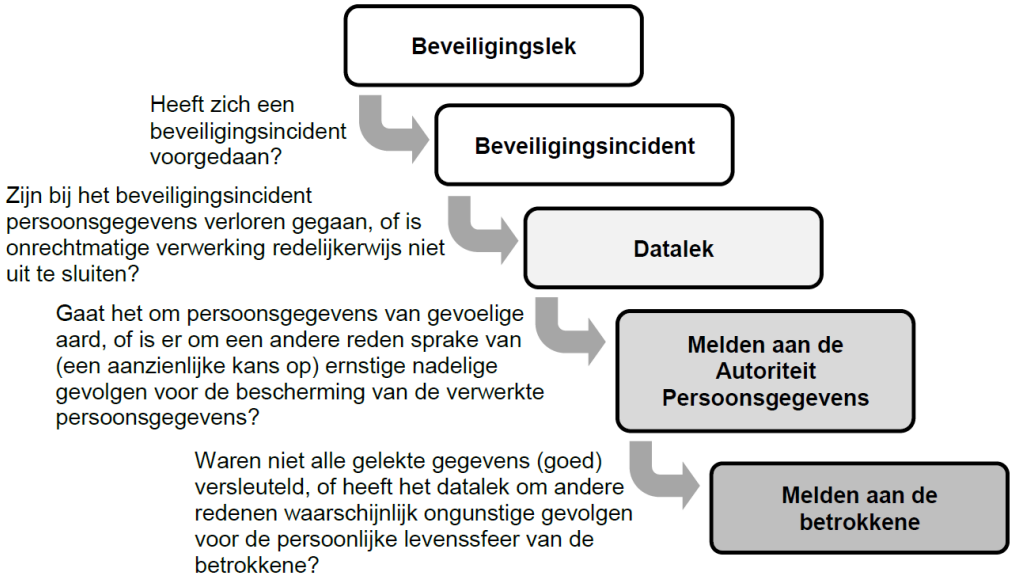
Op 1 januari 2016 gaat de meldplicht datalekken in. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En in een aantal gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Kader

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Hierin staat dat u de persoonsgegevens die u verwerkt moet beveiligen tegen verlies en tegen onrechtmatige verwerking (artikel 13 Wbp). Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).

Afwegingen

Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet u een aantal afwegingen maken. Het onderstaande schema geeft deze afwegingen weer.



Datalek

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Melden aan de Autoriteit Persoonsgegevens

U hoeft niet ieder datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moet u een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard moet u denken aan:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp* Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene* Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens* De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude* Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat u een datalek moet melden waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

U moet de melding doen zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kunt u de melding zo nodig aanvullen of intrekken.

Melden aan betrokkene

Als u tot de conclusie komt dat u een datalek moet melden aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat u dit datalek ook moet melden aan de betrokkene. U moet hiervoor een aparte afweging maken.

De wet geeft aan dat u een melding moet doen aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunt u er in principe van uit gaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

Uw melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. De wet schrijft voor dat u de melding *onverwijld* moet doen. U moet daarbij rekening houden met het feit dat de betrokkene naar aanleiding van uw melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Als u passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene achterwege laten. Bij deze beschermingsmaatregelen moet u bijvoorbeeld denken aan cryptografische bewerkingen zoals encryptie en hashing. U moet per geval bepalen of de maatregelen die u heeft genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

Uitzonderingen op de meldplicht

De meldplicht datalekken uit de Wbp is niet van toepassing als de Wbp niet van toepassing is. Dit is bijvoorbeeld het geval als u uitsluitend voor persoonlijke of huishoudelijke doeleinden persoonsgegevens verwerkt.

Als u een aanbieder van een openbare elektronische communicatiedienst bent, dan heeft u te maken met twee meldplichten voor datalekken: de meldplicht in de Telecommunicatiewet (Tw) en de meldplicht in de Wbp. Valt een datalek (gedeeltelijk) onder de meldplicht datalekken uit de Tw? Ook dan moet u het datalek melden aan de Autoriteit Persoonsgegevens en mogelijk aan de betrokkene. In de Wbp zijn voorzieningen opgenomen om dubbele meldingen te voorkomen.

Als u een financiële onderneming bent zoals bedoeld in de Wet op het financieel toezicht (Wft), dan is de verplichting uit de Wbp om datalekken te melden aan de betrokkene niet op u van toepassing. Als u de betrokkenen informeert, doet u dat op grond van uw zorgplicht als financiële onderneming.

Boete

Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro. Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

4.3 Bijlage: Bronnen & gerelateerde documenten

Inhoud	Verwijzing / bronnen
Algemene informatie & meldingsformulier Datalekken	https://www.autoriteitpersoonsgegevens.nl/
Algemene informatie en best practices informatiebeveiliging voor lokale overheden	https://informatiebeveiliging-gemeenten.nl/
Algemene informatie omtrent informatiebeveiliging lokale overheden (informatiebeveiligingsdienst Nederland)	www.ibdgemeenten.nl
Beleidsregels voor toepassing van artikel 34a van de Wbp inzake De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) d.d. 8 december 2015	Autoriteit Persoonsgegevens, De meldplicht datalekken in de Wbp
Bewerkersovereenkomst Rentree	20161004 - Bewerkersovereenkomst - Rentree - Basissjabloon - v1.3
De Baseline Informatiebeveiliging (woning)Corporaties (BIC), een toepassingshandleiding voor NEN/ISO 27001 en 27002 voor woningcorporaties	BIC, NetwIT
Plan van aanpak	20151212_PvA_Meldingplicht_datalekken.doc, versie 1.0
Handreiking gegevensbescherming, mei 2016	Handreiking gegevensbescherming Aedes
Wbp, wet bescherming persoonsgegevens	http://wetten.overheid.nl/BWBR0011468/2016-01-01#Hoofdstuk2