Melden van datalekken

Deze procedure voorziet in een gestructureerde wijze voor het melden van datalekken in het kader van de Wet bescherming persoonsgegevens (Wbp).

Definities

1. Het kan gebeuren dat gegevens van bedrijven of overheidsorganisaties toegankelijk worden voor mensen die geen recht hebben op kennisname van die gegevens (datalek). Artikel 34a lid 1 van de Wbp zegt dat het gaat om “een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens”. Deze inbreuken dienen “onverwijld” te worden gemeld aan de toezichthouder. Vervolgens zegt artikel 34a lid 2 dat de / alle betrokkenen ook in kennis gesteld moeten worden “indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer”.
2. Boetebevoegdheid: de toezichthouder kan “bestuurlijke boetes” opleggen van “ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht”. Dit is een boete van maximaal € 810.000.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis draagt of krijgt van een privacylek, is verplicht dit direct te melden aan zijn Afdelingshoofd, de Coördinator informatiebeveiliging en de Controller informatiebeveiliging;
2. De Controller informatiebeveiliging is verantwoordelijk voor het onderzoeken van het incident;
3. Het Afdelingshoofd is verantwoordelijk voor het ondernemen van preventieve en repressieve acties;
4. De Controller informatiebeveiliging is verantwoordelijk voor de actualiteit van deze procedure.

Uitvoering

1. De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan zijn Afdelingshoofd, de Coördinator informatiebeveiliging en de Controller informatiebeveiliging;
2. De Controller informatiebeveiliging, eventueel in samenwerking met het afdelingshoofd en de Coördinator informatiebeveiliging of beveiligingsbeheerder van het specifieke vakgebied onderzoeken het incident. Hierbij is aandacht voor de volgende aspecten:
   a. wat is de aard van het privacylek;
   b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
   c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
   d. is de organisatie verwijtbaar;
   e. van het incident wordt een verslag gemaakt en in Corsa vastgelegd;
3. De Controller informatiebeveiliging neemt contact op met het CBP en aan de hand van het verslag wordt uitleg gegeven;
4. Eventuele aanwijzingen van het CBP worden vastgelegd en opgevolgd.

Interne controle

5. Op basis van de, gedurende een jaar, ontvangen meldingen analyseert de Controller informatie-beveiliging deze en stelt een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage;
6. Minimaal jaarlijks beoordeelt Controller informatiebeveiliging of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

1. Toelichting

Met ingang van 1 januari 2016 treedt een wijziging van de Wet bescherming persoonsgegevens (Wbp) in werking die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan het College bescherming persoonsgegevens (CBP), en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt.

De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Hiervoor heeft het CBP ter ondersteuning richtsnoeren opgesteld. Deze richtsnoeren dienen tevens als uitgangspunt voor het CBP bij het toepassen van handhavende maatregelen. Deze richtsnoeren treden in werking met ingang van 1 januari 2016, zijnde de datum van inwerkingtreding van de meldplicht datalekken. De definitief vastgestelde richtsnoeren zullen in Corsa worden opgeslagen/gekoppeld aan deze Procedure meldplicht datalekken.

Onderstaand enige aandachtspunten uit deze richtsnoeren van het CBP.

2. Is de meldplicht datalekken uit de Wbp van toepassing?

1.1 Is er sprake van verwerking van persoonsgegevens?

Als er geen sprake is van verwerking van persoonsgegevens, dan is de meldplicht datalekken niet van toepassing.

Verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare persoon (artikel 1, sub a, Wbp). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

1.2 Wie is de verantwoordelijke voor de verwerking?

De meldplicht datalekken richt zich tot de verantwoordelijke voor de verwerking van persoonsgegevens. Wanneer geen verantwoordelijke, dan is de meldplicht datalekken in principe niet van toepassing.

De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel en wie er beslist over de middelen voor die verwerking. Bij de gemeente is de verantwoordelijkheid het college van burgemeester en wethouders van de gemeente

en in specifieke gevallen de burgemeester of gemeenteraad. Een verantwoordelijke kan een vertegenwoordiger aanwijzen die namens hem de verplichtingen uit de Wbp nakomt. Dit is bij de gemeente Lansingerland de Controller informatiebeveiliging.

1.3 Alleen wanneer de Wbp van toepassing is op de verwerking

De meldplicht datalekken uit de Wbp is uitsluitend van toepassing op verwerkingen waarop de Wbp van toepassing is.

Voor de vraag of de Wbp van toepassing is op een verwerking van persoonsgegevens, zijn met name de aard en de doelstelling van de verwerking van belang. Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de Wbp (zoals het verwerken van persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden, bijvoorbeeld uitnodigingen voor een kerstdiner). Op deze verwerkingen is de meldplicht datalekken niet van toepassing. Bij de gemeente zal veelal sprake zijn van verwerking waarop de Wbp van toepassing is.

1.4 Beoordeling of de meldplicht datalekken uit de Wbp op onze gemeente van toepassing is

De beoordeling of de meldplicht datalekken uit de Wbp op onze gemeente van toepassing is, valt onder de verantwoordelijkheid van de Controller informatiebeveiliging en in samenwerking met JZ.

3. Wat moet ik regelen als ik persoonsgegevens laat verwerken door een bewerker?

Veel verantwoordelijken laten de verwerking van hun persoonsgegevens geheel of gedeeltelijk uitvoeren door een zogeheten bewerker. Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen (artikel 1, sub e, Wbp). Van verwerking door een bewerker is bijvoorbeeld sprake bij het Samenwerkings-verband Vastgoedinformatie Heffing en Waardebepaling (SVHW), een organisatie die voor onze gemeente bijvoorbeeld de OZB-belasting heft.

De Controller informatiebeveiligingsbeleid kan er met vakafdeling, al dan niet in samenwerking met de Coördinator informatiebeveiliging of de beveiligingsbeheerder van het specifieke vakgebied, voor zorgen dat er afspraken gemaakt worden met de bewerker, waardoor er voldoende waarborgen zullen zijn ten aanzien van de naleving van de meldplicht voor datalekken. De bewerker dient de maatregelen te treffen die nodig zijn zodat de gemeente aan de meldplicht voor datalekken kan voldoen (artikel 14, lid 3, sub c, Wbp), waaronder het tijdig en adequaat informeren over de datalekken waarvan hij kennis krijgt. De met de bewerker gemaakte afspraken worden vastgelegd in een bewerkersovereenkomst.

4. Is dit een datalek?

Een datalek wordt in de Wbp gedefinieerd als "een inbreuk op de beveiliging, bedoeld in artikel 13" (artikel 34a, lid 1, Wbp). Uitgangspunt is dat de meldplicht datalekken uit de Wbp van toepassing is op de verwerking waarover het gaat (zie hoofdstuk 2).

Voor de meldplicht datalekken geldt dat er sprake moet zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft. Het is dus niet zo dat een enkele tekortkoming of kwetsbaarheid in de beveiliging tot een melding aan de toezichthouder moet leiden. Wanneer redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet het datalek aan het CBP gemeld worden.

Bij een incident waar sprake kan zijn van een inbreuk zoals bedoeld in artikel 34a, lid 1, Wbp kan worden gedacht aan:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- een malware-besmetting;

- een calamiteit zoals een brand in een datacentrum;
- emails (intern/extern) onbeveiligd die privacygevoelige informatie bevatten (m.n. sociaal domein, publiekszaken).

5. Wie moet dit datalek melden aan het CBP?

5.1 Algemeen

De beoordeling of er een datalek aan het CBP gemeld moet worden respectievelijk of het datalek aan de betrokkene moet worden gemeld valt onder de verantwoordelijkheid van de Controller informatiebeveiligingsbeleid.

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat een inbreuk alleen hoeft te worden gemeld als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, lid 1, Wbp).

5.2 Zijn er persoonsgegevens van gevoelige aard gelekt?

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet in ieder geval gekeken worden naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn (bijvoorbeeld aan gegevens over betalingsachterstanden).

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Voorbeelden hiervan zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, e.d., gegevens over de financiële of economische situatie van de betrokkene (salaris- en betalingsgegevens of gegevens die kunnen worden misbruikt voor (identiteits)fraude zoals kopieën van identiteitsbewijzen en om het burgerservicenummer (bsn).

5.3 Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Naast de (gevoelige) aard van de getroffen gegevens zijn ook de aard en de omvang van de inbreuk van invloed op de kans op ernstige nadelige gevolgen. Zo kunnen beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt zeer grote gevolgen hebben voor de betrokkenen. Zo is bij omvangrijke verwerkingen van de overheid vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken. Wanneer de aard en omvang van de getroffen verwerking voldoet aan het bovenstaande, dan moet er van worden uitgaan dat er (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

5.4 Hoe wordt een datalek aan het CBP gemeld?

Het CBP heeft een webformulier beschikbaar waarmee datalekken kunnen worden gemeld. De Controller informatiebeveiliging is verantwoordelijk voor het melden van een datalek aan het CBP.

Ingeval geen gebruik gemaakt kan worden van het webformulier, dan kunnen de gevraagde gegevens per fax toezenden aan het CBP. Het moet hierbij wel aantoonbaar zijn dat de melding tijdig is gedaan. Het CBP verstuurd vervolgens een ontvangstbev estiging.

5.5 Wanneer moet het datalek aan het CBP gemeld worden?

Een datalek moet onverwijld aan het CBP gemeld worden (artikel 34a, lid 1, Wbp). Wel mag er, na het ontdekken van een mogelijk datalek, enige tijd genomen worden voor nader onderzoek teneinde een onnodige melding te voorkomen.

De termijn voor het melden van het datalek begint te lopen op het moment dat de verantwoordelijke zelf, of een bewerker die is heeft ingeschakeld, op de hoogte raakt van een incident waarbij persoonsgegevens kunnen zijn blootgesteld aan verlies of onrechtmatige verwerking. **Uiterlijk op de tweede werkdag na de ontdekking van het incident** moet een melding bij het CBP worden gedaan, tenzij op dat moment inmiddels al uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Dit betekent dat, wanneer op vrijdag het datalek ontdekt wordt, uiterlijk de dinsdag daarna een melding moet worden gedaan bij het CBP. Wordt het datalek op dinsdag ontdekt, dan moet uiterlijk op de daarop volgende donderdag gemeld worden.

Mogelijk is er op de tweede werkdag na de ontdekking van het datalek nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog worden aangevuld of ingetrokken.

Om datalekken tijdig te kunnen melden zullen goede afspraken moeten worden gemaakt met de bewerkers die worden ingeschakeld, zodat zij de verantwoordelijke tijdig en adequaat informeren over alle relevante incidenten.

6. Welke gegevens moeten worden vastgelegd over dit datalek?

De Controller informatiebeveiliging houdt een overzicht bij van alle datalekken die onder de meldplicht vallen. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan wordt ook de tekst van de kennisgeving aan de betrokkene in het overzicht opgenomen (artikel 34a lid 8 Wbp).

De wet schrijft niet voor hoe lang het overzicht moet worden bewaard. Uitgegaan kan worden van een bewaartermijn van **minimaal een jaar**. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren.

7. Moet het datalek aan de betrokkene worden gemeld?

Wanneer is vastgesteld dat het betreffende datalek gemeld moet worden bij het CBP dient tevens beoordeeld te worden of het datalek aan betrokkene moet worden gemeld. Zo kan kennisgeving aan betrokkenen bijvoorbeeld achterwege blijven wanneer de technische beschermingsmaatregelen die zijn genomen voldoende bescherming biden, of wanneer een datalek waarschijnlijk geen ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkene. De richtsnoeren van het CBP hebben een beslisboom ten aanzien van deze beoordeling. De Controller informatiebeveiliging is verantwoordelijk voor het melden van een datalek aan de betrokkene.

Melden van datalek - formulier melding

Gegevens van de melder:

Naam	
Functie	
Contactgegevens	

Omschrijving van het (bijna) incident:

Datum melding:	
Handtekening melder:	