NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Werkprogramma ‘Meldplicht Datalekken’

Handreiking

Versie 1.0 – Mei 2017

Over deze handreiking – Werkprogramma 'Meldplicht Datalekken'

Voor vragen en opmerkingen kunt u zich wenden tot:
NOREA
Postbus 7984, 1008 AD Amsterdam
telefoon: 020-3010380
e-mail: norea@norea.nl

Meer informatie kunt u vinden op:
www.norea.nl
www.privacy-audit-proof.nl
www.deitauditor.nl

Namens de NOREA Kennisgroep Privacy,
Ir. Jan de Heer RE
Mr.drs. Jan Roodnat RE RA

Inhoud

1 Inleiding

Op 1 januari 2016 is de Meldplicht Datalekken in werking treden. In tegenstelling tot wat de naamgeving doet vermoeden, betreft het geen nieuwe wet, maar is het een uitbreiding van de huidige Wet bescherming persoonsgegevens (Wbp). De Meldplicht Datalekken – als onderdeel van de Wbp – betreft artikel 34a.

De meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens (AP), 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 (MD) 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. De AP heeft beleidsregels & richtsnoeren (zie [1] en [2]) opgesteld om organisaties daarbij te ondersteunen. Deze beleidsregels & richtsnoeren dienen tevens als uitgangspunt voor de AP bij het toepassen van handhavende maatregelen.

Een ieder werkzaam binnen een organisatie (bedrijf danwel overheid) kan een mogelijk datalek constateren. Het datalek zal moeten worden gemeld aan het management van de betreffende organisatie. Het is de verantwoordelijkheid van die betreffende organisatie om passende maatregelen te treffen.

Mede op basis van deze richtsnoeren is onderstaand werkprogramma opgesteld. Het werkprogramma wordt voorafgegaan door een beschouwing over informatiebeveiliging omdat dit een centraal item is in de Wbp waaraan in de MD wordt gerefereerd.

Referenties

1. De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp); https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf
2. CBP Richtsnoeren Beveiliging Persoonsgegevens; https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
3. Baseline Informatiebeveiliging Rijksdienst (BIR) & NEN-ISO/IEC 27001 en 27002; https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/inhoud/baseline-informatiebeveiliging-rijksdienst-bir--nen-iso-iec-27001-en-27002
4. Algemene Verordening Gegevensbescherming (AVG) https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming
5. Uitvoeringswet Algemene verordening gegevensbescherming https://www.internetconsultatie.nl/uitvoeringswetavg

2 Informatiebeveiliging

De beveiliging van persoonsgegevens is een van de verplichtingen die de Wbp oplegt aan de verantwoordelijke voor de verwerking van persoonsgegevens.

Artikel 13 (beveiliging) van de Wbp geeft over informatiebeveiliging het volgende aan:

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

Om tot passende beveiligingsmaatregelen te komen heeft de AP specifieke richtsnoeren opgesteld (zie [2]). De richtsnoeren, beveiliging van persoonsgegevens, geven aan dat op het gebied van informatiebeveiliging de volgende zaken moeten worden gerealiseerd om tot passende maatregelen te komen, zoals de Wbp die voorschrijft:

a. maatregelen treffen op basis van risicoanalyse;
b. beveiligingsstandaarden (bijvoorbeeld de BIR zie [3]) toepassen.

Het treffen van beveiligingsmaatregelen op basis van een risicoanalyse stelt de verantwoordelijke in staat om vast te stellen wat het vereiste beveiligingsniveau is en welke maatregelen uiteindelijk moeten worden getroffen. Bij de overheid is dit bijvoorbeeld Dep V of hoger. Indien sprake is van een niveau hoger dan Dep V dan moeten naast de BIR extra beveiligingsmaatregelen worden getroffen die een passend hoger beveiligingsniveau garanderen.

De Privacy werkgroep wil benadrukken dat organisaties al passende beveiligingsmaatregelen moeten hebben getroffen om aan de privacywetgeving (bestaande Wbp) te voldoen. Sommige beveiligingsmaatregelen hebben echter door de [MD] een groter gewicht gekregen. Dit betreft bijvoorbeeld de BIR-maatregelen met betrekking tot de bewerkersovereenkomst (indien van toepassing).

3 Doelgroep

Onderstaand werkprogramma is primair bedoeld voor (IT) auditors die de status moeten bepalen aangaande de implementatie van de meldplicht datalekken. Het betreft It-auditors die organisaties adviseren danwel ondersteunen inzake de beveiliging van persoonsgegevens en/of de meldplicht.

Het werkprogramma kan ook praktische handvaten bieden voor security officers, privacy officers en functionarissen gegevensbescherming teneinde te onderzoeken in welke mate een organisatie gereed is inzake de meldplicht datalekken.

4 Meldplicht datalekken – context wetgeving

Wbp

De Wbp regelt de algemene privacy- en dataprotectieregels, zoals: wat zijn persoonsgegevens, hoe lang mag je gegevens bewaren en wanneer moet ik een datalek melden? De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de Wbp in Nederland.

De huidige Wbp is gebaseerd op een Europese Richtlijn. De Wbp, die uit 2001 dateert, is de Nederlandse uitwerking van de Europese Privacyrichtlijn uit 1995 (nr. 95/46/EG).

Elke Europese lidstaat heeft op basis van deze richtlijn zijn eigen privacywet opgesteld. Dit betekent dat de privacywetgeving in de verschillenden Europese lidstaten niet helemaal gelijk is. Nederland loopt voorop met zijn eigen meldplicht datalekken (artikel 34a uit de WbP).

AVG

Om de onderlinge verschillen in de Europese landen gelijk te trekken is een Europese privacy verordening ontworpen in de vorm van de General Data Protection (GDPR). In Nederland is deze wet verwoord in de Algemene Verordening Gegevensbescherming (AVG) (zie [4]).

Doel van de Algemene verordening gegevensbescherming (AVG) is verdergaande harmonisatie binnen de EU op het gebied van privacyregelgeving en bescherming van persoonsgegevens. De AVG is in mei 2016 vastgesteld.

De AVG zal op 25 mei 2018 van toepassing zijn en onze huidige Wet bescherming persoons-gegevens (Wbp) gaan vervangen. Een groot deel van de bepalingen in de AVG heeft dan rechtstreekse werking en behoeft geen omzetting meer in nationale wetgeving.

NB. Vanaf dat moment is in de hele Europese Unie één privacyregeling van toepassing zijn – en vanaf 25 mei 2018 zal ook de handhaving van deze wet starten. Deze verordening zal in heel Europa voor dezelfde regels rondom privacy gaan zorgen.

Teneinde de overgang van de Wbp naar de AVG te faciliteren is een Uitvoeringswet Algemene verordening gegevensbescherming op 9 december ter consultatie aangeboden (zie [5]). Ook de Norea heeft input gegeven op de consultatie Uitvoeringswet Algemene verordening gegevens-bescherming.

NB. Indien de gevolgen van de AVG voldoende helder zijn zal het werkprogramma "Meldplicht datalekken" worden aangepast.

5 Werkprogramma “Meldplicht Datalekken”

Bij de uitvoering van het werkprogramma (laatste kolom) is het uitgangspunt dat op 1 centrale plek in een organisatie het inzicht moet bestaan tav de status van de implementatie (en bijbehorende gegevens) inzake de meldplicht datalekken.

Idealiter dient op deze centrale plek het volgende aanwezig te zijn:

- ✓ procesbeschrijvingen en verantwoordelijkheden inzake meldplicht datalekke;
- ✓ overzicht van verwerkingen waarop de MD van toepassing is;
- ✓ afspraken met externe bewerkers van uitbestede verwerkingen waarop de MD van toepassing is;
- ✓ administratie van beveiligingsincidenten, beveiligingsinbreuken, datalekken en meldingen van datalekken aan de AP en eventueel betrokkenen
- ✓ resultaten van onderzoeken naar de beveiliging van verwerkingen waarop de WMD van toepassing is.

Indien het voorgaande inzicht op centraal niveau niet of voor onderdelen niet kan worden gegeven dat is het advies het onderzoek te stoppen voor het deel waarvoor het inzicht ontbreekt op centraal niveau. Vervolgens vindt rapportage plaats aan verantwoordelijk management.

De bij het onderzoek tevens in het werkprogramma ‘geraakte’ Wbp artikelen zijn:

- Artikel 1 t/m 4: [definities], [materiele reikwijdte en toepasselijkheid], [uitsluiting gebieden], [territoriale reikwijdte]
- Artikel 13: [beveiliging]
- Artikel 12: [geheimhouding]
- Artikel 14: [bewerker]
- Artikel 34a: [meldplicht datalekken]

Het werkprogramma “meldplicht datalekken” biedt de mogelijkheid om vast te stellen (*Inventarisatie)* in welke mate de meldplicht datalekken is geïmplementeerd (in samenhang met een aantal beveiliging-gerelateerde artikelen uit de Wbp). Veelal is sprake van ‘ketenproble-matiek’ waar rekening mee moet worden gehouden.

Vervolgens kunnen op basis van het uitgevoerde werkprogramma (additionele) maatregelen geadviseerd worden (*Preventief, Detectief en Responsief).*

Relatie met de PIA – NOREA – Privacy Impact Assessment

De Norea heeft ook een handreiking Privacy Impact Assessment (PIA)opgesteld om in brede zin privacyrisico's (en reducerende maatregelen) in een vroeg stadium op een gestructureerde en heldere manier in beeld te kunnen brengen. Het bepalen van risico's inzake de meldplicht datalekken is ook een onderdeel van de PIA. Het werkprogramma "meldplicht datalekken" richt zich meer in detail op de geïmplementeerde maatregelen om invulling te geven aan de meldplicht (in samenhang met een aantal beveiligingsmaatregelen).

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
Artikel 1 t/m 4 Inventarisatie	1b Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder 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. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten.	Is de meldplicht op de verwerking van toepassing?	De meldplicht datalekken uit de Wbp is van toepassing wanneer aan de volgende voorwaarden wordt voldaan. • Er is sprake van een verwerking van persoonsgegevens. • De organisatie is verantwoordelijke voor de verwerking. • De Wbp is van toepassing op de verwerking. Op basis van bovenstaande vragen zijn de verwerkingen in kaart gebracht waarop de meldplicht van toepassing is.	Stel vast dat de verwerkingen (inclusief aard, locatie en gevoeligheid van de persoonsgegevens) in kaart zijn gebracht waarop de meldplicht van toepassing is en dat hiervoor een procesbeschrijving aanwezig is.	Stel vast dat er een proces-beschrijving is die voorziet in het in kaart brengen van de verwerkingen waarop de meldplicht datalekken van toepassing is. Uit de proces-beschrijving blijken onder andere de volgende criteria: • Er is sprake van een verwerking van persoonsgegevens. • Houdt rekening met 'ketenproblematiek' • De aard, locatie en gevoeligheid van de persoonsgegevens) • De organisatie is verantwoordelijke voor de verwerking. • De Wbp is van toepassing op de verwerking. Stel vast dat er een overzicht is van de verwerkingen (inclusief aard, locatie en gevoeligheid van de persoonsgegevens) waarop de meldplicht datalekken van toepassing is.

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
Artikel 14 lid 3 Inventarisatie	De verantwoordelijke draagt zorg dat de bewerker: a. De persoonsgegevens verwerkt in overeenstemming met artikel 12 eerste lid; b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13, 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.	Wat moet er worden geregeld als persoonsgegevens worden bewerkt door een bewerker ?	Als er persoonsgegevens worden verwerkt door een bewerker, dan moeten er voldoende waarborgen zijn dat door de bewerker aantoonbaar aan de meldplicht voor datalekken wordt voldaan. De wet schrijft niet voor wat er precies met de bewerker moet worden afgesproken. De AP geeft de volgende suggesties. • Gaat de bewerker u daad-werkelijk informeren over alle relevante incidenten? • Treft de bewerker maat-regelen om potentiele datalekken op te sporen en worden eveiligingsincidenten geanalyseerd om datalekken vast te stellen. • Gaat de bewerker eventueel zelf meldingen doen aan de AP? • Ontvangt u per incident alle informatie die u nodig heeft? • Hoe gaat de bewerker u informeren over de incidenten? • Wordt u tijdig geïnformeerd over de incidenten? • Wordt u op de hoogte gehouden van eventuele nieuwe ontwikkelingen rond	Stel vast dat er schriftelijke afspraken met de bewerker zijn gemaakt waarin de suggesties van de AP zoveel mogelijk zijn opgenomen. Stel vast of de bewerkers-overeenkomsten aan de noodzakelijke vereisten voldoen.	Stel vast dat er een procesbeschrijving is die voorziet in het maken van afspraken met externe bewerkers over datalekken. Onderzoek of geregeld is wie de melding doet van een datalek (verantwoordelijke danwel bewerker) aan het AP Stel vast dat voor de verwerkingen waarop de meldplicht datalekken van toepassing is en waarvan beheeractiviteiten zijn in- of uitbesteed met de externe bewerker schriftelijke afspraken zijn gemaakt waarin de suggesties van de AP zijn opgenomen. Stel vast of er in de afgelopen periode (vanaf 1 januari 2016) door de bewerker beveiligings-incidenten, beveiligings-inbreuken danwel datalekken zijn gemeld aan de verantwoordelijke of de AP. Stel vast dat de verantwoordelijke door de bewerker is geïnformeerd over de geïmplementeerde beveiligingsmaatregelen inzake de persoonsgegevens en de werking daarvan

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
			het incident, en van de maatregelen die de bewerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen? • Kunt u vaststellen dat u daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt? • Welke Beveiligingsmaatregelen zijn door de bewerker getroffen? De afspraken met de bewerker over bovenstaande zijn schriftelijk vastgelegd. Een mondelinge afspraak is niet voldoende.		in de afgelopen periode (vanaf 1 januari 2016) .
Artikel 13 Preventie en Detectie	De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoons-gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich	Is sprake van een datalek? Is afhankelijk van de daadwerkelijk getroffen beveiligingsmaat-regelen (“passend” beveiligingsniveau).	Een datalek wordt in de Wbp gedefinieerd als "een inbreuk op de beveiliging, bedoeld in artikel 13 Wbp". Artikel 13 Wbp verplicht de verantwoordelijke om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Een Privacy Impact Assessment kan behulpzaam zijn bij het bepalen van passende beveiligings-maatregelen. Denk bij passende maatregelen ook aan awareness programma’s en encryptie, hashing, remote wipe.	Stel vast dat er voor alle beveiligingsincidenten is bepaald of er sprake is van een datalek. De resultaten van deze analyse dienen te worden vastgelegd ook als uit de analyse bleek dat er geen sprake was van een datalek. Stel ook vast dat hiervoor een	Stel vast dat er procedures zijn gericht op een zo volledig mogelijke registratie van beveiligingsincidenten en datalekken. Daarnaast dienen er maatregelen zijn getroffen zoals het actief monitoren van mogelijke datalekken. Onder actief monitoren wordt verstaan logging, het reageren op meldingen/klachten van bewerkers en andere in/externe meldingen en het (periodiek) gebruik van Pen Testing en Intrusion Detection Tools of het uitvoeren van andere beveiligingsonderzoeken.

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
	meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.		Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Dit betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen of niet. Een datalek kan zich in beide situaties voordoen. Vastgesteld dient derhalve te worden of door een beveiligingsincident de verwerkte persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking en redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt.	procesbeschrijving aanwezig is. Uit deze procesbeschrijving dient met name het verband te blijken tussen primaire registraties (bijvoorbeeld logging en incidenten / klachten), beveiligingsincidenten en datalekken.	Stel vast dat door de verantwoordelijke is vastgesteld dat de geïmplementeerde beveiligingsmaatregelen passend zijn en de afgelopen periode (vanaf 1 januari 2016) hebben gewerkt. Stel vast dat voor alle in de afgelopen periode (vanaf 1 januari 2016) geregistreerde beveiligingsincidenten is bepaald of sprake is van een datalek. Stel vast dat na een datalek afdoende maatregelen zijn getroffen om herhaling te voorkomen.
Artikel 34a lid 1 Respons	De verantwoordelijke stelt de AP onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen	Moet een datalek daadwerkelijk worden gemeld aan de AP?	Een inbreuk hoeft alleen te worden gemeld bij de AP als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Melding bij de AP dient plaats te vinden als er persoonsgegevens van gevoelige	Stel vast dat er een procedure is gericht op het bepalen van de meldingswaardigheid van een datalek. Stel vast dat de relevante datalekken	Stel vast dat er een procedure is aan de hand waarvan gemotiveerd kan worden vastgesteld dat een datalek wel of niet moet worden gemeld aan de AP. Uit de procesbeschrijving blijken onder andere de volgende criteria: • Heeft ernstige nadelige gevolgen voor de bescherming van

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
	heeft voor de bescherming van persoonsgegevens.		aard gelekt en/of de aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. De organisatie dient een procedure/ werkwijze te hebben om te beoordelen of er sprake is van ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Hierbij zijn van belang: • De aard en omvang van de inbreuk. • De aard van de gelekte persoonsgegevens. • De mate waarin organisatorische en technische beschermingsmaatregelen zijn getroffen ten aanzien van de persoonsgegevens. • Hierbij dient aansluiting gezocht te worden met de bestaande incidentprocedure om ervoor te zorgen dat alle inbreuken op de beveiliging in beeld zijn.	zijn gemeld aan de AP.	persoonsgegevens omdat persoonsgegevens van gevoelige aard zijn gelekt en/of. • Kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens als gevolg van de aard en omvang van de inbreuk. • Stel vast dat alle meldingswaardige datalekken in de afgelopen periode (vanaf 1 januari 2016) tijdig zijn gemeld aan de AP.
Artikel 34a lid 2 Respons	De verantwoordelijke stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer.	Moet een datalek worden gemeld aan de betrokkene?	• Datalekken worden in beginsel gemeld aan de betrokkene. Uitzonderingen zijn van toepassing wanneer: • De technische beschermingsmaatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.	Stel vast dat er een procedure is gericht op de meldingswaardigheid van een datalek. Stel vast dat de relevante datalekken zijn gemeld aan betrokkene.	Stel vast dat er een procedure is gericht op het bepalen van de meldingswaardigheid van een datalek aan de betrokkene. Uit de procesbeschrijving blijkt onder andere dat de betrokken wordt geïnformeerd over: • Welke persoonsgegevens op welke wijze (mogelijkerwijze) zijn gelekt

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
			• Dit is in de situatie dat passende technische beschermingsmaatregelen ervoor zorgen dat de persoons-gegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens. • Dit is een strenge norm, die van geval tot geval moet worden toegepast op basis van de actuele stand van de techniek. Als wordt getwijfeld over de adequaatheid van de technische beschermingsmaatregelen die zijn getroffen, dan moet het datalek worden gemeld aan de betrokkene. • Een technische maatregel kan versleuteling (encryptie) zijn. De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Persoonsgegevens kunnen als adequaat versleuteld worden beschouwd als ze: • op een veilige manier zijn versleuteld met een standaardalgoritme, de sleutel niet is gelekt, en de sleutel op zo'n manier is gegenereerd dat onbevoeg-den deze niet kunnen achterhalen met de beschikbare technologische middelen; of op een veilige manier zijn vervangen door een hashwaarde die		• Passende organisatorische en technische beschermingsmaatregelen • Houdt rekening met 'ketenproblematiek' • Mogelijke ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene. • Advies aan betrokkene welke acties hij/zij kan ondernemen om het risico te verminderen. Stel aan de hand van de aan de AP gemelde datalekken vast of alle relevante datalekken in de afgelopen periode (vanaf 1 januari 2016) tijdig aan de betrokkene zijn gemeld.

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
			met een standaardalgoritme is berekend, de sleutel niet is gelekt, en de sleutel op zo'n manier is gegenereerd dat onbevoegden deze niet kunnen achterhalen met de beschikbare technologische middelen. • Het datalek waarschijnlijk geen ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene. • Er zwaarwegende redenen zijn om de melding aan de betrokkene achterwege te laten. Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in dit artikel. • Voor alle aan de AP gemelde datalekken wordt vastgesteld of ook melding aan de betrokkene moet plaatsvinden.		
Artikel 34a lid 3 (en lid 1) Respons	De kennisgeving aan de AP en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de	Hoe en wanneer moet een datalek worden gemeld aan het AP?	**HOE.** De melding aan de AP dient in ieder geval de volgende items te bevatten: Gevolgen van de inbreuk. • Getroffen of voorgestelde maatregelen om gevolgen te verhelpen. • Aanbevolen maatregelen aan betrokkenen om de negatieve gevolgen te beperken.	Stel aan de hand van de ontvangstbeves-tigingen van de AP vast dat de datalekken volledig en tijdig zijn gemeld.	Stel vast dat er procedurebeschrijvingen zijn gericht op het volledig en tijdig melden van datalekken aan de AP. Stel aan de hand van de ontvangstbevestigingen van de AP vast dat alle relevante datalekken in de

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
	negatieve gevolgen van de inbreuk te beperken.		**WANNEER. U**iterlijk op de tweede werkdag (72 uren) na de ontdekking van het incident moet het datalek worden gemeld bij de AP via het daartoe bestemde webformulier van de AP of via de fax. De AP stuurt een ontvangstbevestiging.	Stel vast dat alle relevante items aan de AP zijn gemeld.	afgelopen periode (vanaf 1 januari 2016) volledig en tijdig zijn gemeld.
Artikel 34a lid 4 en 5 Respons	De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.	Hoe en wanneer moet een datalek worden gemeld aan de betrokkene?	**HOE.** In de kennisgeving aan de betrokkene dient het volgende te worden opgenomen • de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen en de maatregelen die de betrokkene worden aanbevolen om te nemen om de negatieve gevolgen van de inbreuk te beperken. • Belangrijk is dat zo veel mogelijk betrokkenen worden bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. • Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt. **WANNEER.** Datalekken dienen onverwijld te worden gemeld aan de betrokkenen. Het onverwijld melden houdt in:	Stel vast dat alle relevante betrokkenen tijdig met voldoende informatie zijn geïnformeerd over de datalekken.	Stel vast dat er procedurebeschrijvingen zijn gericht op het volledig en tijdig melden van datalekken aan de betrokkene. Stel vast dat alle relevante datalekken in de afgelopen periode (vanaf 1 januari 2016) volledig en tijdig zijn gemeld aan betrokkene.

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
			• dat een organisatie, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat de betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd. • Wel moet er rekening mee worden gehouden dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. • Hoe eerder de betrokkene daarover wordt geïnformeerd, hoe eerder deze in actie kan komen. • Net als bij de melding aan de AP kan er eventueel voor worden gekozen om de betrokkene in eerste instantie te informeren op basis van de informatie waarover op dat moment wordt beschikt, zodat deze alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek, en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen.		
Artikel 34a lid 8 Respons	De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige	Welke gegevens moeten worden vastgelegd over een datalek?	Er dient een overzicht te worden bijgehouden van alle datalekken die onder de meldplicht vallen. Per datalek bevat het overzicht in ieder geval feiten en gegevens	Stel vast dat er een overzicht beschikbaar is van alle datalekken die de afgelopen 3	Stel vast dat er een procedurebeschrijving is gericht op het administreren van alle datalekken die onder de meldplicht vallen.

Artikel-nrs.	Meest relevante wettelijke bepalingen voor het toetsingskader	Vraag op basis van de wet	Wat moet er gebeuren bij de verantwoordelijke / functionaris gegevensbescherming	Toetsingskader	Werkprogramma
	gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoons-gegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.		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. Het overzicht wordt minimaal drie jaar bewaard en periodiek (minimaal een maal per jaar) wordt geëvalueerd of het datalek alsnog aan de betrokkene gemeld moet worden.	jaren onder de meldplicht vielen. Stel tevens vast dat de vereiste gegevens in het overzicht zijn opgenomen en dat ieder jaar wordt vastgesteld of alsnog melding aan betrokkenen moet plaatsvinden.	De administratie dient minimaal 3 jaar te worden bewaard en er dient periodiek (minimaal een maal per jaar) te worden geëvalueerd of het datalek alsnog aan de betrokkene gemeld moet worden. Stel vast dat er een administratie is waarin de datalekken van de afgelopen periode (vanaf 1 januari 2016) die onder de meldplicht vallen volledig zijn opgenomen. Stel vast of is nagegaan of er datalekken zijn die alsnog aan betrokkene gemeld moeten worden.

Begrippen

AP
De Autoriteit Persoonsgegevens (opvolger van het College bescherming persoonsgegevens).

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegeven verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Datalek
De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten.

Derde Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke
of de bewerker gemachtigd is om persoonsgegevens te verwerken.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Verantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder 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.

Wbp
De Wet bescherming persoonsgegevens. De nationale uitwerking van de Europese richtlijn 95/46/EC die toeziet op bescherming van persoonsgegevens.