PROCEDURE MELDEN DATALEKKEN O.G.V. DE WET BESCHERMING PERSOONSGEGEVENS GEMEENTE VALKENBURG AAN DE GEUL

Doel
Deze procedure wordt gehanteerd voor het vaststellen en melden van datalekken.

Definities en omschrijving
• Beveiligingsincident: een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 13 van de Wet bescherming persoonsgegevens (Wbp).
• Datalek: beveiligingsincident dat leidt tot een aanzienlijke kans op ernstige nadelige gevolgen of ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
• Melding: kennisgeving van een datalek aan de Autoriteit Persoonsgegevens (AP) en aan de betrokkene(n).

Inleiding
Op 1 januari 2016 is de meldplicht datalekken in de Wbp ingevoerd (Artikel 34a). Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de AP, en in bepaalde gevallen ook aan de betrokkene van wie persoonsgegevens zijn gelekt.
Elk datalek moet worden beoordeeld en de verantwoordelijke moet een afweging maken of het datalek onder het bereik van de meldplicht valt. In deze notitie worden handvatten gegeven voor de beoordeling van het datalek en de melding daarvan.
Het niet voldoen aan de meldplicht kan leiden tot handhaving door de AP. Bij een ernstige schending van de meldplicht kan een boete ter hoogte van € 820.000 worden opgelegd.

De gemeente Valkenburg aan de Geul verwerkt in haar dienstverlenings- en bedrijfsvoeringsprocessen een omvangrijke hoeveelheid persoonsgegevens, niet alleen van burgers maar ook van medewerkers. Op de meeste verwerkingen van persoonsgegevens is de Wbp van toepassing. Artikel 13 van de Wbp bepaalt dat de verantwoordelijke voor de verwerking van persoonsgegevens, meestal het college van burgemeester en wethouders of de burgemeester, passende technische en organisatorische maatregelen treft 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 ook op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Voor de gemeente Valkenburg aan de Geul is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) het uitgangspunt voor de te treffen maatregelen.

Wat is een datalek?
De getroffen maatregelen bieden nooit een volledige garantie dat de beveiliging niet kan worden doorbroken. Een doorbreking van de beveiliging is op zichzelf geen datalek. Er is pas sprake van een datalek als de doorbreking:
1. óf leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens
2. óf ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geïnterpreteerd. 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 beveiligingsmaatregelen had getroffen of niet.
Voorbeelden van beveiligingsincidenten zijn:
• verlies of diefstal van een USB-stick, laptop, mobiele telefoon, tablet etc.
• inbraak door een hacker;
• verzending van een externe e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
• een malware-besmetting (malware is software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen);

• een calamiteit zoals brand in een serverruimte.

Melding bij de Autoriteit Persoonsgegevens (AP)
Indien er sprake is van een ’datalek’, dan moet dit binnen 72 uur nadat het beveiligingsincident aan de verantwoordelijke bekend is gemaakt, gemeld worden bij de AP (en in bepaalde gevallen ook bij de betrokkene(n)). Voor een melding geldt dat er sprake moet zijn van het 'lekken van data' én 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 een melding aan de AP tot gevolg moet hebben. Als de gegevens op de verloren USB-stick of op de gestolen laptop zijn versleuteld, is in principe geen onrechtmatige toegang mogelijk. Dat is wel het geval als een medewerker een tablet verliest met daarop onversleutelde gegevens van klanten met wie de gemeente contacten onderhoudt.
Als redelijkerwijs niet is uit te sluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid of mogelijk kan leiden, dan moet het datalek worden gemeld aan de AP uiterlijk 72 uur na ontdekking van het incident.

Melding aan betrokkene
Volgens de Wbp stelt de verantwoordelijke de betrokkene direct in kennis van de inbreuk op de beveiliging als die inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
De verantwoordelijke moet daarbij een inschatting maken. Ongunstige gevolgen zijn er al snel als een onbevoegde kennis heeft kunnen nemen van de zogenaamde bijzondere gegevens. Dit betreft onder meer medische gegevens, strafrechtgegevens, seksuele leven, godsdienst en levensovertuiging. Deze gegevens zijn privacygevoeliger dan gegevens als naam en geboortedatum en kunnen bij verlies of misbruik ernstige gevolgen hebben voor de betrokkene. In dergelijke gevallen dient de verantwoordelijke de betrokkene in kennis te stellen van het datalek.

Taken, verantwoordelijkheden en bevoegdheden
- De leidinggevenden zorgen er voor dat het thema ‘melding datalekken’ voldoende aandacht krijgt, bijvoorbeeld in het werkoverleg of de terugkoppelingen.
- De privacy en security officer is verantwoordelijk voor de actualiteit van deze procedure, de bekendmaking en het in kennis stellen c.q. instrueren van de medewerkers;
- Iedere medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident, is verplicht dit direct te melden aan zijn/haar direct leidinggevende en de concernjurist;
- De concernjurist is verantwoordelijk voor onderzoek en rapportage naar aanleiding van beveiligingsincident en betrekt hierbij de direct leidinggevende en de privacy en security officer;
- De privacy en security officer is verantwoordelijk voor de advisering van de betrokken direct leidinggevende, eventueel het DT, MT, CMT en het bestuur over de mogelijke gevolgen van een beveiligingsincident voor de privacy van de betrokkene;
- De direct leidinggevende verleent alle medewerking aan het onderzoek en is verantwoordelijk voor het ondernemen van preventieve en repressieve beveiligingsacties;
- De concernjurist is de aangewezen contactpersoon met de AP en daarmee verantwoordelijk voor:
- de melding aan de AP en aan betrokkene;
- de communicatie met de AP en betrokkenen naar aanleiding van de meldingen.

Uitvoering
1. De medewerker die direct of indirect kennis draagt of krijgt van een beveiligingsincident meldt dit direct aan de concernjurist en zijn/haar direct leidinggevende.
2. De concernjurist en zo nodig de beveiligingsbeheerder van het specifieke vakgebied, onderzoeken het beveiligingsincident en betrekken hierbij de direct leidinggevende en de privacy en security officer. Hierbij is aandacht voor de volgende aspecten:
a. wat is de aard van het beveiligingsincident;
b. wat is de oorzaak dat dit beveiligingsincident heeft plaatsgevonden;
c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
d. is er sprake van verwijtbaar handelen en door wie.

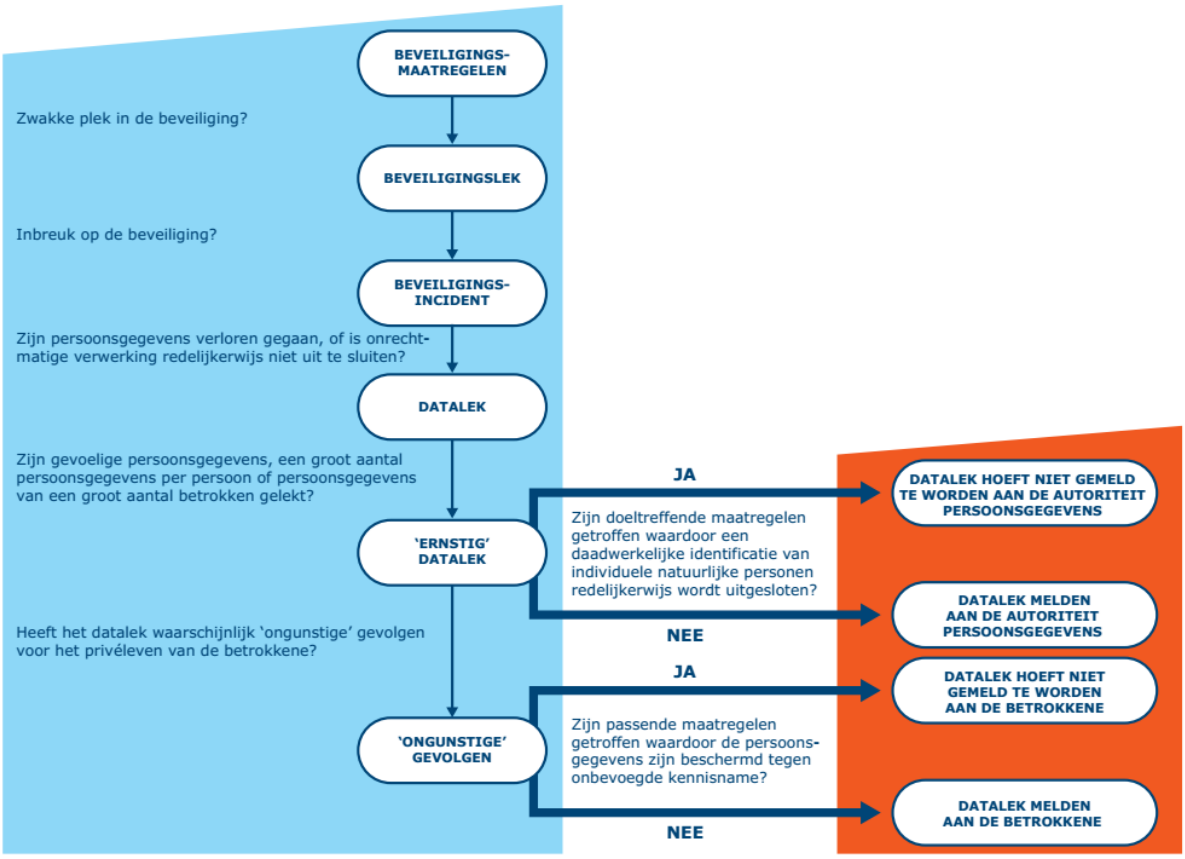
3. De concernjurist maakt van het beveiligingsincident een verslag. Het verslag bevat in ieder geval de volgende informatie:
a. plaats in de organisatie waar het beveiligingsincident zich heeft voorgedaan;
b. op welk informatiesysteem of persoonsgegevens verwerkend proces het beveiligingsincident betrekking heeft;
c. een beschrijving van het beveiligingsincident;
d. opgave van de categorieën van personen waarvan de (bijzondere) persoonsgegevens betrokken zijn in het beveiligingsincident;
e. inzicht in de getroffen maatregelen die genomen zijn om eventuele gevolgen te beperken;
f. inzicht in de getroffen maatregelen om dergelijke beveiligingsincidenten in de toekomst te voorkomen.
4. De concernjurist beoordeelt of het beveiligingsincident ernstige nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n) en adviseert management en bestuur over het doen van de meldingen aan de AP en aan de betrokkene(n);
5. Bestuur en management besluiten over het al dan niet doen van een melding;
6. De concernjurist doet namens de direct leidinggevende de melding aan de AP en aan de betrokkene(n);
7. De concernjurist is aanspreekpunt voor de AP en voorziet de AP voor zover noodzakelijk van nadere toelichting;
8. Eventuele aanwijzingen van de AP worden vastgelegd en opgevolgd;
9. De privacy en security officer legt een dossier aan van het beveiligingsincident en registreert dit in de beveiligingsincidentregistratie;
10. De privacy en security officer informeert de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) over incidenten die gevolgen kunnen hebben voor andere verantwoordelijken.

Bewaren van informatie over datalek
Wanneer een datalek aan de Autoriteit persoonsgegevens wordt gemeld, wordt er een overzicht hiervan bewaard; hiervoor wordt een beveiligingsincidentregistratie ingericht. Dit overzicht bevat de feiten en gegevens van het lek, zoals de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als het datalek ook aan de getroffen personen is gemeld, wordt de communicatie hierover bewaard.
De wet schrijft niet voor hoe lang het overzicht moet worden bewaard. In eerste instantie wordt er uitgegaan van een bewaartermijn van minimaal één jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Zo moeten de gegevens minimaal drie jaar worden bewaard als er geen melding aan de betrokkene is gedaan omdat er zwaarwegende redenen waren of omdat er voldoende technische beschermingsmaatregelen zijn genomen, waardoor er geen ongunstige gevolgen voor de betrokkene zijn.

Interne controle / bijstelling procedure
• De privacy en security officer analyseert de ontvangen meldingen van een jaar, en stelt een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage.
• De privacy en security officer beoordeelt een keer per jaar 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.

Communicatie
• De medewerkers via de nieuwsbrief informeren over de vaststelling van de ‘Procedure melden datalekken’.
• De ‘Procedure melden datalekken’ permanent plaatsen op intranet en daarbij in het bijzonder aandacht vragen voor gebruik en beveiliging van laptop, mobiele telefoon, tablet en thuiswerken.
• De ‘Procedure melden datalekken’ ter kennis van de raad brengen.

Schema beoordeling datalek:



Valkenburg, 21 maart 2017
Burgemeester en wethouders van Valkenburg aan de Geul,

L.T.J.M. Bongarts
algemeen directeur / gemeentesecretaris,

dr. J.J. Schrijen
burgemeester,

Versie 170216

BIJLAGE 1

Gegevens melden datalekken (website Autoriteit Persoonsgegevens)
Deze bijlage bevat de gegevens die opgeven moeten worden als een datalek gemeld wordt aan de Autoriteit Persoonsgegevens. Bij dit formulier zijn de vragen uit de Europese Verordening 611/2013 als uitgangspunt gehanteerd.

Aard van de melding
1. Is dit een vervolg op een eerdere melding? (Kies een van de volgende opties.)
   a. Ja
   b. Nee

2. Wat is het nummer van de oorspronkelijke melding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)

3. Wat is de strekking van de vervolgmelding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties.)
   a. Toevoegen of wijzigen van informatie betreffende de eerdere melding
   b. Intrekking van de eerdere melding

4. Wat is de reden van intrekking? (Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie b.)

Wettelijk kader
5. Op grond van welke wettelijke bepaling doet u deze melding?
   a. Artikel 34a, eerste lid, van de Wbp
   b. Artikel 11.3a, eerste lid, van de Tw

Algemene informatie en contactgegevens
6. Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)
   a. Naam van het bedrijf of de organisatie
   b. (Bezoek)adres
   c. Postcode
   d. Plaats
   e. KvK-nummer

7. Door wie wordt het datalek gemeld? (Vul de onderstaande gegevens in.)
   a. Naam van de persoon die meldt
   b. Functie van de persoon die meldt
   c. E-mailadres van de persoon die meldt
   d. Telefoonnummer van de persoon die meldt
   e. Alternatief telefoonnummer van de persoon die meldt

8. Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding? (Vul de onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek.)
   a. Naam contactpersoon
   b. Functie van de contactpersoon
   c. E-mailadres van de contactpersoon
   d. Telefoonnummer van de contactpersoon
   e. Alternatief telefoonnummer van de contactpersoon

9. In welke sector is het bedrijf of de organisatie actief?
   a. Overheid: gemeente

Gegevens over het datalek

10. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

11. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    a. Minimaal: (vul aan)
    b. Maximaal: (vul aan)

12. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

13. Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
    a. Op (datum)
    b. Tussen (begindatum periode) en (einddatum periode)
    c. Nog niet bekend

14. Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)
    a. Lezen (vertrouwelijkheid)
    b. Kopiëren
    c. Veranderen (integriteit)
    d. Verwijderen of vernietigen (beschikbaarheid)
    e. Diefstal
    f. Nog niet bekend

15. Om welk type persoonsgegevens gaat het? (U kunt meerder mogelijkheden aankruisen.)
    a. Naam-, adres- en woonplaatsgegevens
    b. Telefoonnummers
    c. E-mailadressen of andere adressen voor elektronische communicatie
    d. Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
    e. Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    f. Burgerservicenummer
    g. Paspoortkopieën of kopieën van andere legitimatiebewijzen
    h. Geslacht, geboortedatum en/of leeftijd
    i. Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
    j. Overige gegevens, namelijk (vul aan)

16. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
    a. Stigmatisering of uitsluiting
    b. Schade aan de gezondheid
    c. Blootstelling aan (identiteits)fraude
    d. Blootstelling aan spam of phishing
    e. Anders, namelijk (vul aan)

Vervolgacties naar aanleiding van het datalek

17. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Inlichten van de betrokkenen

18. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)
    a. Ja
    b. Nee
    c. Nog niet bekend

19. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)
    a. Ik heb het datalek aan de betrokkenen gemeld op (datum)
    b. Ik ga het datalek aan de betrokkenen melden op (datum)
    c. Nog niet bekend

20. Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

21. Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

22. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

23. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)
    a. De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
    b. Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)
    c. Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)
    d. Anders, namelijk: (vul aan)

Technische maatregelen

24. Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)
    a. Ja
    b. Nee
    c. Deels, namelijk: (vul aan)

25. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

Internationale aspecten

26. Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
    a.J a
    b. Nee
    c. Nog niet bekend

27. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    a. Ja, namelijk: (vul aan)
    b. Nee

Vervolgmelding

28. Is naar uw mening deze melding compleet? (kies een van de onderstaande opties.)
    a. Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
    b. Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

BIJLAGE 2

Relevante wetsartikelen

Deze bijlage bevat de volledige tekst van de geciteerde wetsartikelen.

Artikel 1 Wbp

a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

b. 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;

c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

e. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

f. betrokkene: degene op wie een persoonsgegeven betrekking heeft;

g. 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;

h. ontvanger: degene aan wie de persoonsgegevens worden verstrekt;

i. toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;

j. Onze Minister: Onze Minister van Veiligheid en Justitie;

k. het College bescherming persoonsgegevens of het College: het College als bedoeld in artikel 51;

l. functionaris: de functionaris voor de gegevensbescherming als bedoeld in artikel 62;

m. voorafgaand onderzoek: een onderzoek als bedoeld in artikel 31;

n. verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;

o. verzamelen van persoonsgegevens: het verkrijgen van persoonsgegevens;

p. de Kaderwet: de Kaderwet zelfstandige bestuursorganen;

q. bindende aanwijzing: de zelfstandige last die wegens een overtreding wordt opgelegd;

r. zelfstandige last: de enkele last tot het verrichten van bepaalde handelingen, bedoeld in artikel 5:2, tweede lid, van de Algemene wet bestuursrecht, ter bevordering van de naleving van wettelijke voorschriften.

Artikel 2 Wbp

1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze wet is niet van toepassing op verwerking van persoonsgegevens:

a. ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden;

b. door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002;

c. ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012;

d. die is geregeld bij of krachtens de Wet basisregistratie personen;

e. ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens en

f. ten behoeve van de uitvoering van de Kieswet.

3. Deze wet is niet van toepassing op verwerking van persoonsgegevens door de krijgsmacht indien Onze Minister van Defensie daartoe beslist met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde. Van de beslissing wordt zo spoedig mogelijk mededeling gedaan aan het College.

Artikel 4 Wbp

1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.

2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.

3. Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke.

Artikel 13 Wbp

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.

Artikel 14 Wbp

1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de 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. De verantwoordelijke ziet toe op de naleving van die maatregelen.

2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

3. 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.

4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b en c.

5. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, de beveiligingsmaatregelen, bedoeld in artikel 13, en de 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, schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

Artikel 34a Wbp

1. De verantwoordelijke stelt het College 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 heeft voor de bescherming van persoonsgegevens.

2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

3. De kennisgeving aan het College 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 negatieve gevolgen van de inbreuk te beperken.

4. De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

5. 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.

6. Het tweede lid is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.

8. De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. 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.

9. Dit artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.

10. Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.

11. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.

Artikel 43 Wbp

De verantwoordelijke kan de artikelen 9, eerste lid, 30, derde lid, 33, 34, 34a, tweede lid, en 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van:

a. de veiligheid van de staat;

b. de voorkoming, opsporing en vervolging van strafbare feiten;

c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;

d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of

e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Artikel 51 Wbp

1. Er is een College bescherming persoonsgegevens dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Tevens houdt het College toezicht op de verwerking van persoonsgegevens in Nederland, wanneer de verwerking plaatsvindt overeenkomstig het recht van een ander land van de Europese Unie.

2. Het College wordt om advies gevraagd over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens.

3. De Kaderwet is van toepassing op het College, behoudens de in deze wet genoemde uitzonderingen.

4. Het College wordt in het maatschappelijk verkeer aangeduid als: Autoriteit persoonsgegevens.

Artikel 51a Wbp

1. Het College is bevoegd om in het belang van een efficiënt en effectief toezicht op de verwerking van persoonsgegevens afspraken te maken met andere toezichthouders en daartoe gezamenlijk met deze toezichthouders samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.

2. Het College en de toezichthouders, bedoeld in het eerste lid, zijn bevoegd uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens betreffende de verwerking van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun taak.

Artikel 60 Wbp

1. Het College kan ambtshalve of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.

2. Het College brengt zijn voorlopige bevindingen ter kennis van de verantwoordelijke of de groep van verantwoordelijken die bij het onderzoek zijn betrokken en stelt hen in de gelegenheid hun zienswijze daarop te geven. Houden de voorlopige bevindingen verband met de uitvoering van enige wet, dan brengt het College deze tevens ter kennis van Onze Minister die het aangaat.

3. In geval van een onderzoek, ingesteld op verzoek van een belanghebbende, doet het College aan deze mededeling van zijn bevindingen, tenzij zodanige mededeling onverenigbaar is met het doel van de gegevensverwerking of de aard van de persoonsgegevens, dan wel gewichtige belangen van anderen dan de verzoeker, de verantwoordelijke daaronder begrepen, daardoor onevenredig zouden worden geschaad. Indien het mededeling van zijn bevindingen achterwege laat, zendt het de belanghebbende zodanig bericht als hem geraden voorkomt.

Artikel 62 Wbp

Een verantwoordelijke of een organisatie waarbij verantwoordelijken zijn aangesloten kan een eigen functionaris voor de gegevensbescherming benoemen, onverminderd de bevoegdheden van het College ingevolge hoofdstuk 9 en 10 van deze wet.

Artikel 63 Wbp

1. Als functionaris kan slechts worden benoemd een natuurlijke persoon die voor de vervulling van zijn taak over toereikende kennis beschikt en voldoende betrouwbaar kan worden geacht.

2. De functionaris kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Hij ondervindt geen nadeel van de uitoefening van zijn taak. De verantwoordelijke stelt de functionaris in de gelegenheid zijn taak naar behoren te vervullen. De functionaris kan de kantonrechter verzoeken te bepalen dat de verantwoordelijke gevolg dient te geven aan hetgeen in de tweede volzin is bepaald.

3. De functionaris oefent zijn taken eerst uit nadat de verantwoordelijke of de organisatie die hem heeft benoemd, hem heeft aangemeld bij het College. Het College houdt een lijst bij van aangemelde functionarissen.

4. De functionaris is verplicht tot geheimhouding van hetgeen hem op grond van een klacht of een verzoek van betrokkene is bekend geworden, tenzij de betrokkene in bekendmaking toestemt.

Artikel 64 Wbp

1. De functionaris ziet toe op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Het toezicht strekt zich uit tot de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd of door de verantwoordelijken die zijn aangesloten bij de organisatie die hem heeft benoemd.

2. Indien op de verwerking een krachtens artikel 25 vastgestelde gedragscode van toepassing is, strekt het toezicht mede uit tot de naleving van deze code.

3. De verantwoordelijke of de organisatie als bedoeld in het eerste lid draagt zorg dat de functionaris ter vervulling van zijn taak over bevoegdheden beschikt die gelijkwaardig zijn aan de bevoegdheden zoals geregeld in Titel 5.2 van de Algemene wet bestuursrecht.

4 De functionaris kan aanbevelingen doen aan de verantwoordelijke die strekken tot een betere bescherming van de gegevens die worden verwerkt. In gevallen van twijfel overlegt hij met het

Artikel 65 Wbp

Het College is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de bij of krachtens deze wet gestelde verplichtingen.

Artikel 66 Wbp

1. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht ter zake van overtreding van het bepaalde bij of krachtens de artikelen 4, derde lid, of 78, tweede lid, aanhef en onder a.

2. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht ter zake van overtreding van het bepaalde bij of krachtens de artikelen 6 tot en met 8, 9, eerste en vierde lid, 10, eerste lid, 11 tot en met 13, 16, 24, 33, 34, eerste, tweede en derde lid, 34a, 35, eerste lid, tweede volzin, tweede, derde en vierde lid, 36, tweede, derde en vierde lid, 38 tot en met 40, tweede en derde lid, 41, tweede en derde lid, 42, eerste en vierde lid, 76, 77 of 78, derde en vierde lid, alsmede van artikel 5:20 van de Algemene wet bestuursrecht. Artikel 23, zevende lid, van het Wetboek van Strafrecht is van overeenkomstige toepassing.

3. Het College legt geen bestuurlijke boete op wegens overtreding van het bepaalde bij of krachtens de in artikel 66, tweede lid, genoemde artikelen, dan nadat het een bindende aanwijzing heeft gegeven. Het College kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.

4. Het derde lid is niet van toepassing indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.

5. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht in geval van niet-nakoming van een bindende aanwijzing. Artikel 23, zevende lid, van het Wetboek van Strafrecht is van overeenkomstige toepassing.