Onze organisatie en de Algemene Verordening Gegevensbeheer

2018

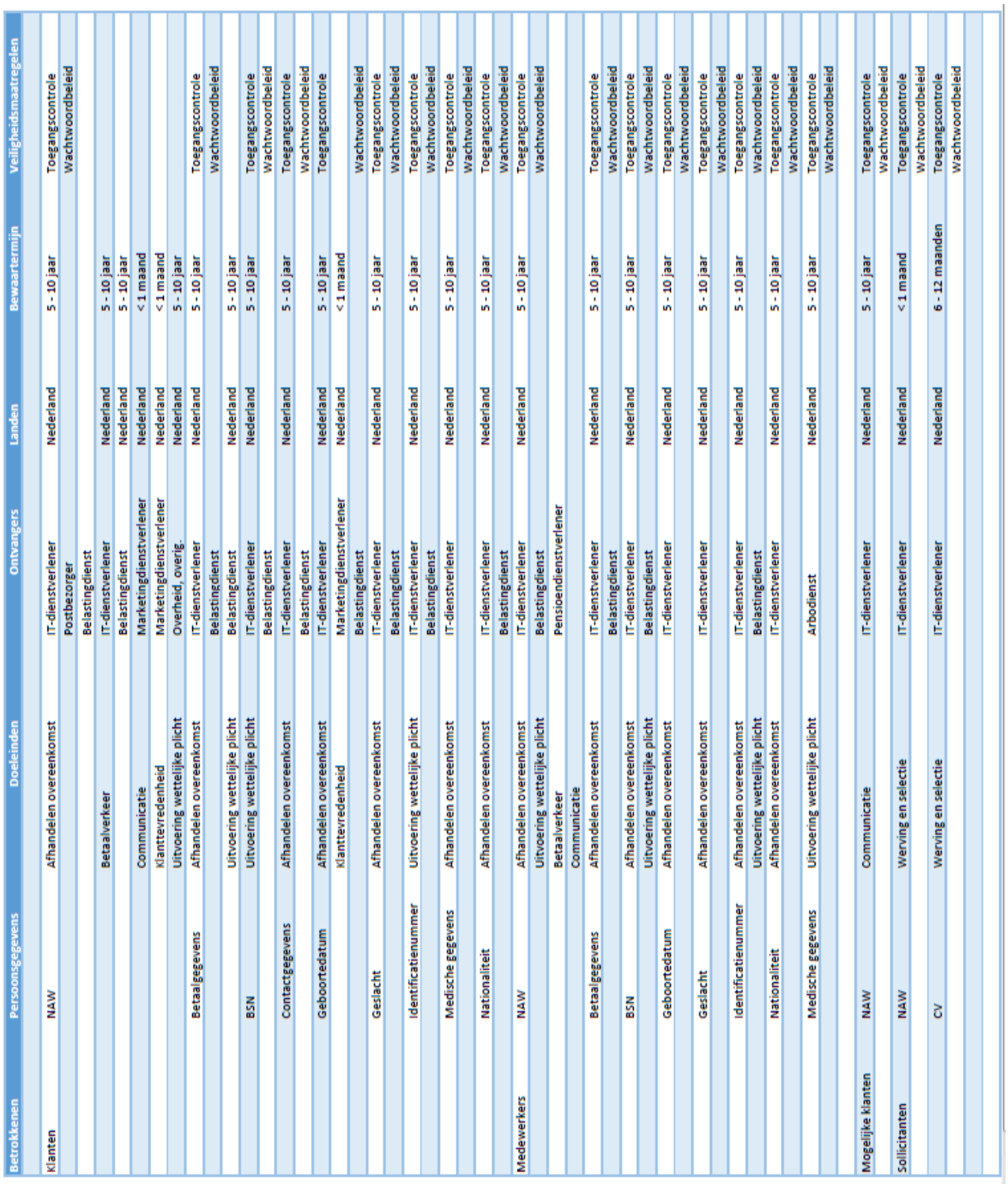
Inhoud

Inleiding

De Algemene Verordening Gegevensbescherming is de nieuwe privacywet voor heel Europa. Vanaf 25 mei 2018 moeten organisaties voldoen aan deze wet. Het doel van deze wet is de bescherming van persoonsgegevens. Voor onze organisatie betekent dit dat wij heel concreet hebben gekeken naar ons gegevensbeheer, onze gegevensstromen en beveiliging. Dit alles hebben wij beschreven in dit document. Dit document is daarmee een naslagwerk geworden, maar daarnaast ook een levend document. Als organisatie willen wij de gegevensbescherming serieus nemen en hebben wij een actieplan opgesteld hoe wij op korte termijn nog meer kunnen voldoen aan de AVG.

1. Verwerkingsregister

Het verwerkingsregister is een document wat verwerkt wordt door de AO rol binnen onze organisatie. Het excel bestand is daarom bij de persoon die deze rol vervuld in beheer. Hieronder een afbeelding van het huidige verwerkingsregister.



Betrokkenen	Persoonsgegevens	Doeleinden	Ontvangers	Landen	Bewaartermijn	Veiligheidsmaatregelen
Klanten	NAW	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Postbezorger			Wachtwoordbeleid
			Belastingdienst			
		Betaalverkeer	IT-dienstverlener	Nederland	5 - 10 jaar	
			Belastingdienst	Nederland	5 - 10 jaar	
		Communicatie	Marketingdienstverlener	Nederland	< 1 maand	
		Klanttevredenheid	Marketingdienstverlener	Nederland	< 1 maand	
		Uitvoering wettelijke plicht	Overheid, overig.	Nederland	5 - 10 jaar	
	Betaalgegevens	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
		Uitvoering wettelijke plicht	Belastingdienst	Nederland	5 - 10 jaar	
	BSN	Uitvoering wettelijke plicht	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
	Contactgegevens	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
	Geboortedatum	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
		Klanttevredenheid	Marketingdienstverlener	Nederland	< 1 maand	
			Belastingdienst			Wachtwoordbeleid
	Geslacht	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
	Identificatienummer	Uitvoering wettelijke plicht	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
	Medische gegevens	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
	Nationaliteit	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
Medewerkers	NAW	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
		Uitvoering wettelijke plicht	Belastingdienst			Wachtwoordbeleid
		Betaalverkeer	Pensioendienstverlener			
		Communicatie				
	Betaalgegevens	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
			Belastingdienst			Wachtwoordbeleid
	BSN	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
		Uitvoering wettelijke plicht	Belastingdienst			Wachtwoordbeleid
	Geboortedatum	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
	Geslacht	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
	Identificatienummer	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
		Uitvoering wettelijke plicht	Belastingdienst			Wachtwoordbeleid
	Nationaliteit	Afhandelen overeenkomst	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
	Medische gegevens	Uitvoering wettelijke plicht	Arbodienst	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
Mogelijke klanten	NAW	Communicatie	IT-dienstverlener	Nederland	5 - 10 jaar	Toegangscontrole
						Wachtwoordbeleid
Sollicitanten	NAW	Werving en selectie	IT-dienstverlener	Nederland	< 1 maand	Toegangscontrole
						Wachtwoordbeleid
	CV	Werving en selectie	IT-dienstverlener	Nederland	6 - 12 maanden	Toegangscontrole
						Wachtwoordbeleid

2. Privacy verklaring

De onderstaande privacy verklaring staat op onze website.

Privacyverklaring

25 mei 2018

Uw privacy is voor ons van groot belang. Wij houden ons dan ook aan de privacywet. Dit betekent dat uw gegevens veilig zijn bij ons en dat wij ze altijd netjes gebruiken. In deze privacyverklaring leggen we uit wat we bij de website allemaal doen met informatie die we over u te weten komen.

Als u vragen hebt, of wilt weten wat we precies van u bijhouden, neem dan contact op met de hoofdbegeleid(ster) van de betreffende locatie.

Contactformulier en Nieuwsbrief
Met het contactformulier kunt u ons vragen stellen of aanvragen doen.

Hiervoor gebruiken wij uw e-mailadres en naw-gegevens. Deze hebben wij nodig vanwege het contract die we met u sluiten. Wij bewaren deze informatie totdat we zeker weten dat u tevreden bent met onze reactie.

U kunt zich abonneren op onze nieuwsbrief. Hierin leest u nieuwtjes, tips en informatie over onze producten en diensten. Dit abonnement kunt u op ieder moment opzeggen. Iedere nieuwsbrief bevat een afmeldlink.
Uw e-mailadres wordt alleen met uw toestemming toegevoegd aan de lijst van abonnees. Deze gegevens worden bewaard totdat u het abonnement opzegt.

Memo
Wij willen u graag informatie sturen over praktische zaken en nieuwe producten of diensten. Dit doen wij per e-mail. U kunt op ieder moment bezwaar maken tegen deze communicatie.

Verstrekking aan andere bedrijven of instellingen
Met uitzondering van de hierboven genoemde partners, geven wij uw persoonsgegevens onder geen voorwaarde aan andere bedrijven of instellingen, behalve als wij dat wettelijk verplicht zijn (bijvoorbeeld als de politie dat eist bij een vermoeden van een misdrijf).

In onze website zijn social media buttons opgenomen. Hiermee verzamelen de beheerders van deze diensten uw persoonsgegevens.

Google Analytics
Wij gebruiken Google Analytics om bij te houden hoe bezoekers onze website gebruiken. Wij hebben een verwerkersovereenkomst met Google gesloten. Daarin staan strikte afspraken te maken over wat zij mogen bijhouden. Wij hebben Google niet toegestaan de verkregen Analytics informatie te gebruiken voor andere Google diensten. Wij laten Google de IP-adressen anonimiseren.

Beveiliging
Beveiliging van persoonsgegevens is voor ons van groot belang. Om uw privacy te beschermen, nemen wij de volgende maatregelen:

- *Toegang tot persoonsgegevens wordt afgeschermd met een gebruikersnaam en wachtwoord- Toegang tot persoonsgegevens wordt afgeschermd met een gebruikersnaam en een login token*

Wijzigingen in deze privacyverklaring
Wanneer onze website wijzigt, moeten wij natuurlijk ook de privacyverklaring aanpassen. Let dus altijd op de datum hierboven en kijk regelmatig of er nieuwe versies zijn. Wij zullen ons best doen wijzigingen ook apart aan te kondigen.

Inzage, wijzigen en verwijderen van uw gegevens
Als u vragen hebt of wilt weten welke persoonsgegevens wij van u hebben, kunt u altijd contact met ons opnemen..

U hebt de volgende rechten:

- *uitleg krijgen over welke persoonsgegevens we hebben en wat we daarmee doen*
- *inzage in de precieze persoonsgegevens die we hebben*
- *het laten corrigeren van fouten*
- *het laten verwijderen van verouderde persoonsgegevens*
- *intrekken van toestemming*
- *bezwaar maken tegen een bepaald gebruik*

Let op dat u altijd duidelijk aangeeft wie u bent, zodat we zeker weten dat we geen gegevens van de verkeerde persoon aanpassen of verwijderen.

Klacht indienen
Als u vindt dat wij u niet op de juiste manier helpen, dan heeft u het recht om een klacht in te dienen bij de toezichthouder. Deze heet de Autoriteit Persoonsgegevens.

3. Privacy protocol

3.1 Welke gegevens verzamelen wij

Binnen onze organisatie hebben wij te maken met persoonsgegevens. De gegevens die wij verzamelen hebben te maken met een overeenkomst die wij sluiten met personen. Dit zijn klanten, maar dat zijn ook medewerkers. De gegevens van onze klanten hebben wij nodig om de overeenkomst te kunnen afhandelen, betaalverkeer mogelijk te maken, voor communicatie doeleinden, klanttevredenheid en ook vanuit een wettelijke verplichting. De gegevens van onze medewerkers hebben wij oa nodig voor bovenstaande punten. Naast de gegevens van klanten en medewerkers hebben wij ook te maken met gegevens van mogelijke klanten en van sollicitanten. Deze groep is kleiner, maar daarom niet minder belangrijk. Wij zijn ons bewust van de waarde van de persoonsgegevens en gaan daarom zorgvuldig om met deze gegevens. In dit document wordt verteld hoe wij binnen onze organisatie dienen om te gaan met deze gegevens.

3.2 Hoe informeren wij onze klanten over ons gegevensbeheer

Op onze website staat een privacy verklaring. In deze privacyverklaring staat nauwkeurig beschreven waar wij gegevens voor gebruiken. Het is van groot belang dat een ieder zelf kan aangeven hier wel of niet toestemming voor te willen geven. Een privacyverklaring wordt ook opgenomen in het contract met onze klant. Op die manier kan een klant aangeven of deze toestemming wil verlenen voor het gebruik van de gegevens.

3.3 Waar worden de gegevens bewaard

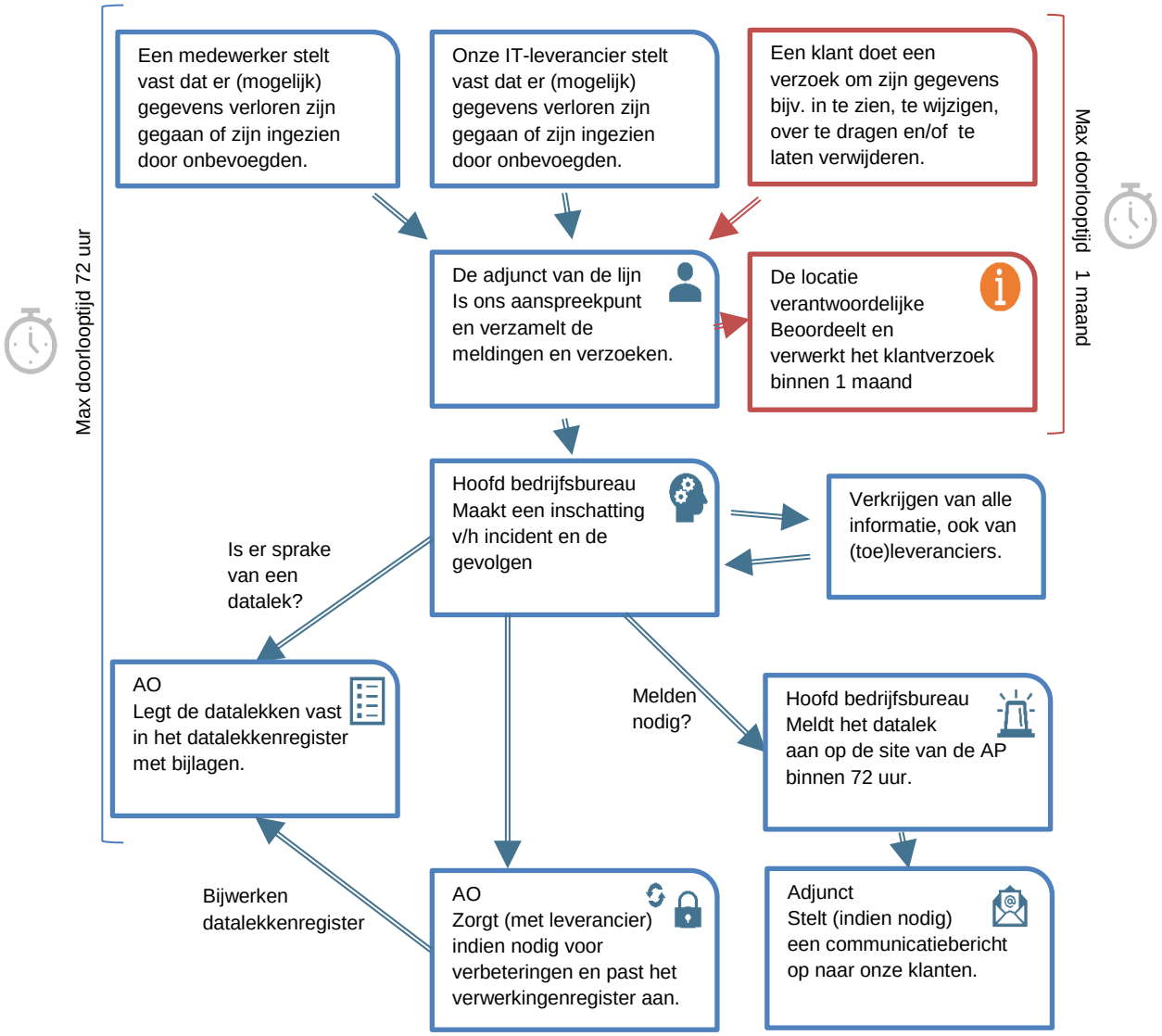
Onze organisatie werkt met een digitale werkomgeving. Binnen deze werkomgeving is er een mappenstructuur waarin gegevens worden beheerd door locatie verantwoordelijken. De plek waar de meeste persoonsgegevens aanwezig zijn, is in de administratie systemen. Met de leveranciers van deze systemen hebben wij een overeenkomst hoe de privacy geborgd is. In het verwerkingsregister staat hoelang wij bepaalde gegevens bewaren.

3.4 Wie heeft er toegang tot de gegevens en hoe is dit beveiligd

Er zijn verschillende rollen binnen onze organisatie die toegang hebben tot verschillende soorten gegevens. Er is een duidelijk overzicht welke rol bepaalde rechten heeft en daarmee toegang tot bepaalde gegevens. De rollen en de bijbehorende rechten zijn duidelijk verwoord binnen onze organisatie en weggezet in rolprofielen. De rechten worden beheerd bij degene die de rol AO vervuld. Deze persoon is binnen onze organisatie gemachtigd om op elk gewenst moment rechten en of wachtwoorden aan te passen. Bij het krijgen van een wachtwoord krijgt de betreffende medewerker het bericht dat deze persoonlijk is en niet overdraagbaar. Hiermee voorkomen wij dat medewerkers elkaar gegevens kunnen gebruiken. Bij het einde van een diensteverband van een medewerker met bepaalde rechten wordt het wachtwoord direct gewijzigd.

Zoals eerder aangegeven werken wij in een digitale werkomgeving. Daarmee zorgen wij dat opslaan op een computer of harde schijf niet nodig is. Op dit moment inventariseren wij alle hardware en wordt bepaald welke aanpassingen/ vervangingen gedaan moeten worden. Hiermee zorgen wij ervoor dat de hardware veilig genoeg is.

3.5 Intern proces



4. Calamiteitenplan datalekken

Datum: 25-05-2018
Versie: 1

1. Inleiding

In de huidige privacywetgeving (Wet bescherming persoonsgegevens, Wbp) is een meldplicht datalekken opgenomen. Deze meldplicht verplicht organisaties om datalekken te melden bij de toezichthouder (de Autoriteit Persoonsgegevens) en, in sommige gevallen, ook bij de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben, bijvoorbeeld leden, abonnees en/of medewerkers). Ook onder de Algemene Verordening Gegevensbescherming (AVG), die vanaf 25 mei 2018 van toepassing zal zijn, moeten datalekken gemeld worden.

In dit calamiteitenplan wordt omschreven op welke manier onze organisatie omgaat met eventuele datalekken. In het plan is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie verantwoordelijk is voor welke melding en hoe en in welke vorm de melding aan de toezichthouder en eventueel ook aan de betrokkenen wordt gedaan.

In dit beleidsplan worden de beleidsregels van de Autoriteit Persoonsgegevens vertaald naar praktisch en werkbaar beleid voor onze organisatie.

Mochten toekomstige (wettelijke) wijzigingen/veranderingen aanpassing van dit document noodzakelijk maken, dan zal de verantwoordelijke binnen onze organisatie deze aanpassing doorvoeren en het versienummer updaten.

2. Wat is een datalek?

2.1. Introductie

Niet alle datalekken moeten gemeld worden aan de toezichthouder. Een datalek dat wel gemeld dient te worden aan de toezichthouder wordt als volgt omschreven:

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.

Onder de Algemene Verordening Gegevensbescherming (AVG), die vanaf 25 mei 2018 de Wbp zal vervangen, wordt gesproken van een ‘inbreuk in verband met persoonsgegevens’. Dit is “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens”. Een inbreuk hoeft niet te worden gemeld wanneer het onwaarschijnlijk is dat deze redelijkerwijs een risico voor betrokkenen met zich meebrengt.

Om te inventariseren of iets een datalek is, zullen de volgende vragen in deze volgorde moeten worden beantwoord:

1. Is er sprake van een inbreuk op de beveiliging (’beveiligingsincident’)?
2. Zijn er bij de inbreuk persoonsgegevens verloren gegaan?
3. Kan er redelijkerwijs worden uitgesloten dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt?

Iedere vraag is een stap in de beslissing of er sprake is van een datalek. Deze stappen zullen hieronder worden toegelicht.

2.2. Inbreuk op de beveiliging

Van een inbreuk op beveiliging is sprake wanneer zich daadwerkelijk een incident heeft voorgedaan. Alleen een dreiging van een inbreuk op de beveiliging is daarom nog geen incident.

Voorbeelden van beveiligingsincidenten zijn:

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Een inbreuk op de beveiliging wordt vervolgens een datalek wanneer de inbreuk gevolgen heeft voor de persoonsgegevens die onze organisatie verwerkt.

2.3. Verlies van persoonsgegevens

Indien er door de inbreuk op de beveiliging persoonsgegevens verloren zijn gegaan waar geen complete en actuele reservekopie meer van is, is dit altijd te kwalificeren als een datalek.

Voorbeeld: Wanneer een database met klantgegevens door een fout van een programmeur of een medewerker van onze organisatie *wordt vernietigd, en er geen back-up van deze gegevens is, is er sprake van datalek.*

2.4. Onrechtmatige verwerking

Het is echter ook mogelijk dat gegevens onrechtmatig zijn verwerkt. Dit houdt bijvoorbeeld in dat onbevoegde personen toegang hebben verkregen tot gegevens waar zij geen toegang toe mochten hebben. Andere vormen van onrechtmatige verwerking zijn het onrechtmatig wijzigen/aantasten van persoonsgegevens en het verstrekken van persoonsgegevens aan onbevoegden. Het is in dat geval aan onze organisatie om aan te tonen dat iemand de gegevens niet heeft in kunnen zien, of er niets mee gedaan heeft.

Wanneer onze organisatie niet uit kan sluiten dat er persoonsgegevens verloren zijn gegaan, of onrechtmatig zijn verwerkt, is er sprake van een datalek.

Voorbeeld: Als een medewerker van onze organisatie *zijn wachtwoord van zijn e-mailbox op een briefje heeft geschreven en dit briefje kwijt is geraakt, kan dit een datalek zijn als* onze organisatie *niet uit kan sluiten dat onbevoegden toegang hebben verkregen tot de e-mailbox van de medewerker.*
Kan onze organisatie *dit echter wel uitsluiten, bijvoorbeeld door het wachtwoord direct te resetten en in de logfiles te zien dat er in de tussentijd niemand heeft ingelogd, dan is dit geen datalek.*

---

3. Wanneer moet het lek gemeld worden aan de toezichthouder

3.1. Introductie

Op het moment dat er sprake is van een datalek zoals omschreven in hoofdstuk 2, dan is het aan onze organisatie om per vastgesteld datalek te beoordelen of het datalek aan de toezichthouder gemeld moet worden. De toezichthouder stelt dat een datalek aan haar gemeld moet worden indien “er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens”.

Hieronder wordt dit criterium nader uitgewerkt.

3.2. Kwantitatief ernstig

Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig). Zo zal een lek in één van de databases van onze organisatie, waardoor gegevens van bijvoorbeeld 1.000 leden van onze organisatie op straat komen te liggen, kwantitatief ernstig zijn en dus gemeld moeten worden aan de toezichthouder.

3.3. Kwalitatief ernstig

Daarnaast kan een lek ook ernstig zijn indien er geen grote hoeveelheden persoonsgegevens gelekt zijn, maar het wel om gevoelige persoonsgegevens gaat (kwalitatief ernstig). Een paar voorbeelden van wat gevoelige persoonsgegevens zijn:

- inloggegevens;
- financiële gegevens;
- kopieën van identiteitsbewijzen;
- strafrechtelijke gegevens;
- gegevens die betrekking hebben op werkprestaties;
- gegevens die betrekking hebben op levensovertuiging;
- gegevens die betrekking hebben op gezondheid.

De aard en omvang van het datalek dienen telkens in overweging genomen te worden bij de afweging of een lek aan de toezichthouder gemeld dient te worden. Vast staat in ieder geval dat zodra er inloggegevens zijn gelekt, dit te allen tijde gemeld zal moeten worden aan de toezichthouder vanwege de kwalitatieve ernst hiervan.

Voorbeeld: door een lek in de database van onze organisatie *hebben onbevoegden korte tijd inzage in de gegevens van klanten, inclusief hun achterstallige betalingen. Een dergelijk lek van gevoelige gegevens dient aan de toezichthouder gemeld te worden.*

3.4. Termijn

Het datalek dient zo snel mogelijk, maar uiterlijk binnen 72 uur, aan de Autoriteit Persoonsgegevens gemeld te worden. Deze termijn start op het moment dat onze organisatie, of één van haar bewerkers, op de hoogte raakt van het datalek. Een bewerker is een partij die ten behoeve van onze organisatie persoonsgegevens verwerkt. Dit kan bijvoorbeeld de host van de website of een softwareleverancier zijn.

3.5. Waar te melden?

Een datalek dient via de website van de toezichthouder te worden doorgegeven. Dit kan via het meldloket op de website van de Autoriteit Persoonsgegevens. Bij dit invulformulier dienen diverse gegevens ingevuld te worden. Deze worden in hoofdstuk 4 nader uiteengezet.

4. Wat te melden aan de toezichthouder?

De Autoriteit Persoonsgegevens wil specifieke informatie ontvangen indien er sprake is van een datalek dat gemeld dient te worden. Onderstaand is deze vereiste informatie uiteengezet.

Over onze organisatie

- Naam van het bedrijf
- (Bezoek)adres
- Postcode

- Plaats
- KvK-nummer
- Sector waarbinnen onze organisatie actief is

Over de contactpersoon en melder

- Naam
- Functie
- E-mailadres
- Telefoonnummer en alternatief telefoonnummer

Over het datalek

1. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
2. Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie (de bewerker)?
    - Ja, namelijk:
    - Nee
3. Naam van de organisatie waaraan de verwerking is uitbesteed.
4. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    - Minimaal: (vul aan)
    - Maximaal: (vul aan)
5. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
6. Is het bekend wanneer de inbreuk plaats vond?
7. Is de exacte datum bekend wanneer de inbreuk plaats vond?
8. Exacte datum waarop de inbreuk plaats vond.
9. Startdatum van de periode waarbinnen de inbreuk plaats heeft gevonden.
10. Einddatum van de periode waarbinnen de inbreuk plaats heeft gevonden.
11. Wanneer werd de breuk ontdekt?
12. Wat is de aard van de inbreuk? (Meerdere antwoorden mogelijk.)
    - Lezen (vertrouwelijkheid)
    - Kopiëren
    - Veranderen (integriteit)
    - Verwijderen of vernietigen (beschikbaarheid)
    - Diefstal
    - Nog niet bekend
13. Om welk type persoonsgegevens gaat het? (meerdere antwoorden mogelijk)
    - Naam-, adres- en woonplaatsgegevens
    - Telefoonnummers
    - E-mailadressen of andere adressen voor elektronische communicatie
    - Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of lidnummer)
    - Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    - Burgerservicenummer (BSN)
    - Paspoortkopieën of kopieën van andere legitimatiebewijzen
    - Geslacht, geboortedatum en/of leeftijd
    - Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
    - Overige/onbekende gegevens, namelijk (vul aan)
14. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (Meerdere antwoorden mogelijk.)
    - Stigmatisering of uitsluiting

- Schade aan de gezondheid
- Blootstelling aan (identiteits)fraude
- Blootstelling aan spam of phishing
- Anders, namelijk (vul aan)

15. Welke technische en organisatorische maatregelen heeft onze organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
16. Heeft onze organisatie het datalek gemeld aan de betrokkenen of is onze organisatie van plan dat te gaan doen?
    - Ja
    - Nee
    - Nog niet bekend

Vraag 17 tot en met 20 dienen uitsluitend beantwoord te worden indien er een melding aan de betrokkenen gedaan dient te worden:

17. Wanneer heeft onze organisatie het datalek gemeld aan de betrokkenen, of wanneer gaat onze organisatie dit doen?
    - Onze organisatie heeft het datalek aan de betrokkenen gemeld op (datum)
    - Onze organisatie zal het datalek aan de betrokkenen melden op (datum)
    - Nog niet bekend
18. Wat is de inhoud van de melding aan de betrokkenen?
19. Hoe veel betrokkenen heeft onze organisatie in kennis gesteld of gaat onze organisatie in kennis stellen?
20. Welk communicatiemiddel of welke communicatiemiddelen gebruikt onze organisatie of gaat onze organisatie gebruiken bij het in kennis stellen van de betrokkenen?
21. Waarom ziet onze organisatie af van het melden van het datalek aan de betrokkenen?
    - De technische beschermingsmaatregelen die onze organisatie heeft getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
    - Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)
    - Onze organisatie heeft zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)
    - Anders, namelijk: (vul aan)
22. 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.)
    - Ja
    - Nee
    - Deels, namelijk: (vul aan)
23. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Als onze organisatie gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.
24. Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
    - Ja
    - Nee
    - Nog niet bekend
25. Heeft onze organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    - Ja, namelijk: (vul aan)
    - Nee

Na het doen van een melding bij de toezichthouder, wordt er een bevestiging van deze melding toegestuurd naar het e-mailadres van de opgegeven contactpersoon. In deze bevestiging staat tevens het nummer van de melding vermeld, dat noodzakelijk is om een melding te wijzigen en/of

in te trekken.

5. Wanneer moet het lek worden gemeld aan de betrokkenen?

5.1. Introductie

Het kan mogelijk zijn dat een datalek niet alleen aan de toezichthouder, maar ook aan de personen van wie de gegevens zijn gelekt (de betrokkenen) gemeld moet worden. Dit is het geval wanneer het datalek waarschijnlijk ongunstige gevolgen heeft voor het privéleven van deze personen. Hetzelfde geldt uiteraard indien er gegevens van medewerkers van onze organisatie zijn gelekt.

5.2. Ongunstige gevolgen

Een datalek heeft ongunstige gevolgen wanneer het privéleven van de betrokkenen door het lek wordt geschaad. Voorbeelden van dergelijke gevolgen zijn:

- onrechtmatige publicatie;
- aantasting in eer en goede naam;
- identiteitsfraude;
- discriminatie;
- stigmatisering of uitsluiting;
- schade aan de gezondheid;
- reputatieschade.

Als het gaat om persoonsgegevens van gevoelige aard, dan dient er altijd een melding aan betrokkenen gedaan te worden (tenzij er sprake is van adequate beveiliging, zoals omschreven in de volgende paragraaf). Dit betekent bijvoorbeeld, dat zodra er financiële gegevens worden gelekt die niet adequaat zijn beveiligd, hiervan te allen tijde melding aan de betreffende personen zal moeten worden gedaan.

Voorbeeld: een medewerker van onze organisatie *laat sollicitatiebrieven en CV's in een auto liggen en deze auto wordt gestolen. Identiteitsfraude met behulp van deze CV's is niet uit te sluiten en dus is een melding aan de betrokkenen verplicht.*

5.3. Encryptie en hashing

Een datalek hoeft niet aan de betrokkenen gemeld te worden indien de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Hiervan is bijvoorbeeld sprake als de persoonsgegevens voorzien zijn van een beveiliging die volgens de laatste stand van de techniek als 'veilig' kan worden aangemerkt. Denk hierbij bijvoorbeeld aan algemeen gebruikte vormen van encryptie of hashing.

Wanneer het datalek niet hoeft te worden gemeld aan de betrokkenen omdat de gegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan zal wel van tijd tot tijd moeten worden beoordeeld of de gegevens nog steeds onbegrijpelijk of ontoegankelijk zijn (zie ook hoofdstuk 7). Wanneer bijvoorbeeld niet hoeft te worden gemeld (omdat de gegevens encrypted zijn), maar de gebruikte encryptie na anderhalf jaar gecompromitteerd zou raken, moeten de betrokkenen dus alsnog worden ingelicht over het datalek. Er kan ook voor worden gekozen om de betrokkenen direct na het datalek tóch proactief te informeren. Zo wordt voorkomen dat ruime tijd na het datalek betrokkenen alsnog op de hoogte moeten worden gesteld.

Let op: encryptie of hashing biedt echter geen bescherming tegen vernietiging van persoonsgegevens. In dergelijke gevallen dient er dus altijd een melding gedaan te worden aan de betrokkenen als de vernietiging ongunstige gevolgen voor hen heeft.

5.4. Termijn

Het datalek dient ‘onverwijld’ na ontdekking aan de betrokkenen gemeld te worden. ‘Onverwijld’ wil zeggen: zo spoedig als mogelijk, waarbij enige tijd mag worden genomen om de juiste informatie te verzamelen om een zorgvuldige melding te kunnen doen. Met andere woorden: de melding aan de betrokkene moet zorgvuldig gebeuren, maar mag niet onnodig worden vertraagd. De wetgeving koppelt hier geen ‘harde’ termijn aan, zoals bij de melding aan de toezichthouder wel het geval is.Het is de verantwoordelijke die de melding aan betrokkenen doet, tenzij anders afgesproken.

6. Wat te melden aan de betrokkenen?

De melding aan betrokkenen, dient in ieder geval behoorlijk en zorgvuldig uitgevoerd te worden, en de volgende informatie te bevatten:

- Aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
- Waar men terecht kan met vragen, denk hierbij aan het telefoonnummer van de klantenservice of een speciaal telefoonnummer/e-mailadres voor vragen;
- Aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

Het volgende algemene formulier kan als template worden gebruikt. Uiteraard is het daarbij verstandig om in een begeleidend schrijven de betrokkene excuses aan te bieden en duidelijk te maken dat onze organisatie het datalek inmiddels heeft gedicht en er alles aan zal doen om dergelijke gevallen in de toekomst te voorkomen

Melding datalek

Omschrijving	Op [DATUM] heeft er bij ons een datalek plaatsgevonden waarbij mogelijk uw gegevens betrokken zijn.
Vragen?	Voor vragen kunt u contact opnemen met [NAAM] via, [EMAIL] of [TELEFOON].
Wat kunt u doen?	Om de gevolgen van dit datalek te beperken raden wij u aan om [MAATREGELEN].

Uitgangspunt bij het doen van een dergelijke melding is dat dit op individuele basis dient te gebeuren. Als er bijvoorbeeld gegevens van klanten zijn gelekt, dan dient iedere klant hierover apart geïnformeerd te worden. Heeft een datalek een dusdanige omvang dat er een grotere groep wordt getroffen, dan kan er een e-mail rondgestuurd worden naar deze personen met het feit dat er een lek heeft plaatsgevonden. Vervolgens kan er in de e-mail een link opgenomen worden naar een pagina op de website waar meer informatie wordt verstrekt.

Een enkel bericht in de media is niet voldoende om betrokkenen te informeren.

Als uitgangspunt geldt dat wanneer de betrokkenen individueel op de hoogte kunnen worden gesteld, de melding op individuele basis moet plaatsvinden. Pas als dat écht niet haalbaar is, vanwege de omvang van de groep of vanwege het feit dat niet meer te achterhalen is welke personen wel of niet zijn geraakt door het datalek, kan naar andere manieren van informeren worden gekeken.

7. Administratie

Wanneer een datalek aan de toezichthouder is gemeld, dient een overzicht hiervan, zoals hierboven omschreven in hoofdstuk 4, in de administratie bewaard te worden. Onder de toekomstige wetgeving (de Algemene Verordening Gegevensbescherming, die vanaf 25 mei 2018 van toepassing zal zijn), moeten alle datalekken geregistreerd worden, ook de datalekken die niet gemeld hoeven te worden.
De minimale bewaartermijnen zijn door de Autoriteit Persoonsgegevens als volgt vastgesteld:

- Eén jaar wanneer er sprake is van een datalek met ongunstige gevolgen voor betrokkenen;
- Drie jaar wanneer de gelekte gegevens voldoende beveiligd zijn óf wanneer er zwaarwegende belangen zijn om het datalek niet aan betrokkenen te melden. Gedurende deze drie jaar dient gecontroleerd te worden of, indien de gegevens voldoende waren beveiligd, deze beveiliging nog steeds afdoende is of dat het lek ondertussen alsnog gemeld dient te worden aan de betrokkenen.

Deze administratie dient voor de volgende doeleinden bewaard te worden:

- Leren van het datalek;
- Vragen van betrokkenen en derden beantwoorden;
- Alsnog een melding aan betrokkenen doen, wanneer dit na verloop van tijd toch nodig blijkt.

Voorbeeld: Een database met persoonsgegevens is voor korte tijd, door een hack, openbaar geweest. De persoonsgegevens in de database waren volgens de meest recente encryptiestandaard versleuteld en derhalve niet leesbaar voor mensen zonder de juiste autorisaties.

Na een half jaar blijkt echter dat de gebruikte encryptievorm door voortschrijdend inzicht achterhaald is. In dat geval zal er alsnog een melding aan de betrokkenen gedaan moeten worden van het datalek dat een half jaar geleden heeft plaatsgevonden.

NB: De administratie hoeft overigens niet openbaar gemaakt te worden.

8. Melding

8.1. Introductie

Een datalek kan binnen de eigen organisatie ontstaan, maar ook bij een door onze organisatie ingeschakelde derde (denk hierbij aan de leverancier van een CRM-systeem, de hoster, een ingeschakeld marketingbureau etc.). Wanneer een datalek zich voordoet, zal vastgesteld moeten worden waar het datalek zich heeft voorgedaan en hoe dit datalek uiteindelijk bij de toezichthouder en betrokkenen gemeld zal worden.

Dit zal bij onze organisatie in eerste instantie de taak zijn van de adjunct (Directeur of adjunct). De contactgegevens van de directeur of de adjunct zijn opgenomen in paragraaf 8.5.

Uiteraard is het daarbij van belang dat alle betrokken personen, dus zowel het personeel van onze organisatie als het personeel bij de ingeschakelde derden, een datalek kunnen identificeren. Het creëren van bewustzijn binnen het personeel van onze organisatie is dan ook van groot belang. De ontdekker zal een incident te allen tijde moeten melden bij de hierboven genoemde persoon.

8.2. Intern datalek

Wanneer er binnen de eigen organisatie een datalek plaatsvindt, zal iedereen moeten weten hoe er gehandeld dient te worden zodat de melding van het datalek tijdig de juiste personen, en uiteindelijk de toezichthouder en betrokkenen bereikt.

Voor deze situatie dient het volgende pad te worden doorlopen. De ontdekker is degene die een (vermoedelijk) lek detecteert; dat kan iedere willekeurige medewerker van onze organisatie zijn. De ontdekker meldt het lek aan de adjunct (Directeur of adjunct), waarop deze in overleg zal treden met Hoofd Bedrijfsbureau . Naar aanleiding van dit overleg zal er worden besloten of het datalek al dan niet wordt gemeld.

Registratie
Aan de directeur of de adjunct registreert de melding van de ontdekker. De volgende gegevens worden geregistreerd:

- Wie heeft er gemeld?

- Wat is er gemeld?
- Waar kwam de melding vandaan?
- Om welke data (gegevens) gaat het?
- Hoe heeft het incident plaatsgevonden (welke drager is bijvoorbeeld verloren)?
- Welke systemen zijn betrokken/geraakt door het incident?
- Wanneer heeft het incident plaatsgevonden?
- Wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Informeren directie
Indien de directeur of de adjunct het incident kwalificeert als een datalek dat gemeld moet worden, stelt zij Hoofd Bedrijfsbureau mondeling en/of per mail op de hoogte van de volgende informatie:

- omschrijving van het incident (intern/extern datalek);
- de bij het incident betrokken gegevens;
- de achtergrond van de kwalificatie van het incident (waarom is het wel/geen datalek dat gemeld moet worden);
- de (mogelijke) gevolgen;
- wie er reeds zijn geïnformeerd;
- de te nemen vervolgstappen (melding aan de toezichthouder/betrokkenen).

Vervolgens zal besloten worden of het lek wordt gemeld aan de toezichthouder en de betrokkenen. Wanneer het datalek is gemeld aan de toezichthouder en/of de betrokkenen, dan zal de rol AO zorgen voor de juiste interne administratie van het datalek (zie hoofdstuk 7).

8.3. Extern datalek

Een datalek kan ook buiten de organisatie van onze organisatie plaatsvinden. Persoonsgegevens worden tenslotte met derde partijen gedeeld. Denk hierbij aan softwareleveranciers, partijen die ten behoeve van onze organisatie websites leveren of ondersteunen bij de opslag van persoonsgegevens. Wanneer er bij deze derden een datalek plaatsvindt dient dit zo spoedig mogelijk aan onze organisatie gemeld te worden. Momenteel hebben deze derden een zorgplicht om een lek waarvan zij op de hoogte zijn, bij onze organisatie te melden. Onder de AVG wordt deze plicht ook expliciet benoemd.

In bewerkersovereenkomsten met deze derden dienen hier afspraken over vastgelegd te worden. Per externe partij dient onze organisatie een vast contactpersoon te hebben om deze meldingen zo snel en gestroomlijnd mogelijk te laten verlopen. Onderstaande algemene schematische weergave geeft aan hoe een dergelijke melding dient te gebeuren. Dit kan dezelfde persoon zijn die binnen onze organisatie wordt aangewezen als ‘meldpunt’ bij beveiligingsincidenten en/of datalekken, namelijk de adjunct, of de contactpersoon van de betreffende derde partij die dit vervolgens intern zal doorgeven.

8.4. Melden aan betrokkenen

Als een datalek bij onze organisatie bekend is, zal bepaald moeten worden op welke manier de melding, indien vereist, aan de betrokkenen (bijvoorbeeld leden) wordt gedaan. Dit calamiteitenplan kan daarbij als handleiding gebruikt worden.

8.5. Contactgegevens

De volgende contactgegevens zijn van belang indien een datalek zich heeft voorgedaan. Neem altijd direct contact op met de directeur of de adjunct.

5. Verwerkersovereenkomst

Onze organisatie heeft een verwerkersovereenkomst gesloten met de partijen waarmee persoonlijke gegevens worden uitgewisseld. Deze overeenkomsten zijn in het beheer van degene die de rol AO vervuld binnen onze organisatie. Indien noodzakelijk of gewenst is dit op te vragen en in te zien bij de AO' er van onze organisatie.

6. Actieplan

Onze organisatie hecht veel waarde aan het zorgvuldig omgaan van gegevens van personen. Wij zullen om dit reden dan ook dit document blijven updaten wanneer nodig. Ook zijn wij tot de conclusie gekomen dat wij nog niet geheel voldoen aan alle punten. Om die reden hebben wij een aantal concrete acties uitgezet en zullen wij op korte termijn evalueren waar wij nog meer in kunnen verbeteren.

Concrete acties:
Nieuwe werkomgeving in de vorm van office 365. Door office 365 te gebruiken maken wij gebruik van alle gegevens op een digitale omgeving. De toegang wordt strenger bewaakt en rechten kunnen nog bewuster worden toegekend. Het beheer van de rechten en toegangscontrole hoeft niet meer te worden uitbesteed aan derden maar is geheel in eigen beheer. Binnen onze organisatie is dit 1 medewerker die dit beheerd. Op dit moment zijn wij bezig met de implementatie van office 365 binnen onze organisatie. Wij verwachten dat voor het einde van 2018 dit is voltooid.

De websites die we hebben zullen wij aanpassen zodat zij volledig kunnen voldoen aan de AVG. Dit betekent dat er een aanpassing komt of wellicht een volledige vernieuwing. Gezien de omvang van dit project verwachten wij ook hierbij dat het voor het einde van 2018 is voltooid.

De hardware die wij gebruiken op de verschillende locaties zullen wellicht moeten worden vervangen om de veiligheid te kunnen waarborgen. Wij zijn een inventarisatie begonnen om te kunnen bepalen waar er aanpassingen gedaan moeten worden en/ of vervanging noodzakelijk is. Dit is volop in proces en verwachten we voor het einde van 2018 voltooid te hebben.

De bewustwording van de AVG is een belangrijk onderdeel van de werkoverleggen binnen onze organisatie. Om die reden zal dit als vast agendapunt bij de diverse werkoverleggen voorbij komen. Tijdens deze overleggen wordt er aandacht besteed aan uitleg, draagkracht en verantwoordelijkheid. We hopen hiermee de implementatie van de AVG binnen onze organisatie te borgen.