LANDELIJK STIMULERINGSNETWERK THUIS ADMINISTRATIE

LSTA Infosheet Thema: Wet Bescherming Persoonsgegevens

25 januari 2017

Het is met de opkomst van de informatietechnologie steeds gemakkelijker geworden om informatie te verzamelen en te delen. Tegelijkertijd zijn hier ook risico's aan verbonden: de schending van privacy kan vergaande gevolgen hebben.

Persoonsgegevens zijn gegevens aan de hand waarvan een persoon kan worden geïdentificeerd. Veel organisaties verwerken persoonsgegevens. Dit gebeurt ook bij thuisadministratie: al bij de aanmelding en intake worden gegevens over de hulpvrager verzameld. Bovendien wordt binnen thuisadministratie met zeer privacygevoelige informatie gewerkt, namelijk over de financiën van de hulpvrager.

Tot op zekere hoogte is het onvermijdelijk om persoonsgegevens te verzamelen en te verwerken. Maar om de privacy van personen te beschermen zijn er ook regels: het is bijvoorbeeld niet toegestaan om zonder toestemming een foto van iemand op een website te plaatsen. De belangrijkste regels voor het omgaan met persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp) [1].

In dit infosheet wordt eerst ingegaan op de wettelijke bepalingen die van toepassing zijn op de bescherming van persoonsgegevens. Vervolgens wordt ingegaan op de vertaling van de wetgeving naar de praktijk: hoe vind je de optimale balans tussen privacybescherming en werkbare ondersteuning van hulpvragers? Welke maatregelen kunnen genomen worden om de gegevens passend te beschermen?

Inhoud:

1. Wet bescherming persoonsgegevens

Persoonsgegevens zijn alle gegevens aan de hand waarvan een persoon kan worden geïdentificeerd: Naam- en adresgegevens, e-mailadressen, pasfoto's, vingerafdrukken en bijvoorbeeld IP-adressen. Persoonsgegevens zijn ook gegevens die een waardering geven over een persoon, bijvoorbeeld iemands IQ.
Onder *verwerking* van persoonsgegevens wordt verstaan élke handeling met betrekking tot persoons-gegevens[2]. Het laten zien van gegevens aan een externe helpdesk is bijvoorbeeld een verwerking, maar ook het raadplegen of ordenen van gegevens. Er is dus al gauw sprake van het verwerken van persoonsgegevens.
Degene die het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt, is volgens de wet 'de verantwoordelijke'. Dit kan zowel een natuurlijk persoon zijn als een rechtspersoon (de stichting of vereniging) of het bestuur.

[1] De Wbp is sinds 2001 van kracht en is de Nederlandse uitwerking van de Europese Privacyrichtlijn uit 1995. Op basis van deze richtlijn heeft elk Europees lidstaad zijn eigen privacywet opgesteld. In 2018 zal de Algemene Verordening Gegevensbescherming (AVG) in werking treden, waarop in de hele Europese Unie één privacyregeling van toepassing zal zijn. Deze AVG is al ontworpen en goedgekeurd.
[2] De wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens (Wbp artikel 1b).

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

De Wbp is niet van toepassing op verwerking van persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden (art. 2.2.a). De wet geldt wel bij thuisadministratie. Een dienst thuisadministratie is onderdeel van een (hulpverlenende) organisatie, en daarmee is thuisadministratie dus niet meer *uitsluitend* huishoudelijk. De doeleinden zijn ook van hulpverlenende aard. De vrijwilliger die bij de hulpvrager thuis komt, is onderdeel van de organisatie die thuisadministratie aanbiedt. Er wordt informatie over de hulpvragers opgeslagen en/of gedeeld tussen de coördinator en vrijwilligers. Ook worden persoonsgegevens uitgewisseld bij het doorverwijzen van hulpvragers.

De belangrijkste bepalingen uit de Wet bescherming persoonsgegevens zijn:

- **Zorgvuldigheid**
Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.

- **Omschreven doelen en alleen als het écht nodig is**
Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De gegevens mogen vervolgens alleen verder worden verwerkt voor deze doeleinden en moeten toereikend, ter zake dienend en niet bovenmatig zijn.

- **Verplichte informatieverstrekking aan betrokkene**
Degene van wie persoonsgegevens worden verwerkt (*de betrokkene*) moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (*de verantwoordelijke*) en van het doel van de gegevensverwerking.

- Rechtvaardigingsgrond
Voor elke verwerking van persoonsgegevens moet tenminste één rechtvaardigingsgrond aanwezig zijn. Het geven van uitdrukkelijke toestemming door de betrokkene voor het verwerken van zijn/haar persoonsgegevens is zo'n rechtvaardigingsgrond. Andere rechtvaardigingsgronden die in de wet staan zijn bijvoorbeeld het nakomen van een wettelijke verplichting of het bestrijden van een ernstige gezondheidsbedreiging voor de betrokkene.

- **Bewerkersovereenkomst**
Als de verantwoordelijke persoonsgegevens laat verwerken door een bewerker, is een bewerkers-overeenkomst tussen beide verplicht. Dit gaat om externe partijen die bewerkingen uitvoeren in opdracht van de verantwoordelijke.
De vrijwilligers zijn onderdeel van de organisatie die thuisadministratie aanbiedt. Met hen hoeft dus geen bewerkersovereenkomst te worden opgesteld.

- **Beveiliging van persoonsgegevens**
De gegevensverwerking moet op een passende manier worden beveiligd. Hierop wordt later in dit infosheet verder ingegaan. De wet kent ook *bijzondere persoonsgegevens***:** dit zijn extra gevoelige gegevens waarvoor extra strenge regels gelden[3].

- **Rechten van betrokkenen**
Degene van wie de gegevens worden verwerkt heeft inzagerecht en kan een verzoek tot correctie indienen. Tegen bepaalde vormen van gegevensverwerking kan de betrokkene zich verzetten.

Kopietje paspoort verboden!
Bijzondere persoonsgegevens mogen alleen onder strenge voorwaarden worden verwerkt. Het maken van een kopie of scan van zulke gegevens, dus ook van een paspoort, is dan ook in de meeste gevallen verboden.

[3] Dit zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan aantasten: gegevens die iets zeggen over iemands gezondheid, ras, godsdienst of levensovertuiging, politieke gezindheid, strafrechtelijk verleden, seksuele leven, lidmaatschap van een vakvereniging of het BSN.

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

De hulpvrager moet toestemming geven voor het verwerken van zijn/haar persoonsgegevens. Het is dus van belang om de hulpvrager al tijdens het eerste contact te informeren over wat de dienst thuisadministratie precies doet en daarbij uit te leggen welke gegevens voor de vrijwilliger en/of de coördinator voor welke doelen noodzakelijk zijn om bij te houden of te delen (en met wie). De hulpvrager moet snappen waarom bepaalde gegevens nodig zijn om de ondersteuning te kunnen bieden. Leg ook uit dat met de gegevens niet méér dan het noodzakelijke wordt gedaan, hoe lang ze worden bewaard en wat er gedaan wordt om onzorgvuldig gebruik van de gegevens te voorkomen.

Meldingsplicht Wbp

Organisaties die persoonsgegevens verwerken zijn wettelijk verplicht dit te melden bij de Autoriteit Persoonsgegevens, de toezichthouder op het naleven van de Wbp. Er is hiervoor wel een vrijstellingsbesluit van kracht, onder andere voor verenigingen of stichtingen, mits aan bepaalde eisen wordt voldaan[4]: het gaat dan om verwerkingen die veel voorkomen, standaard zijn, met waarborgen omkleed zijn en waarvan algemeen bekend is dat deze plaatsvinden. Het mag bijvoorbeeld alleen gaan om basis persoonsgegevens zoals naam, geslacht, geboortedatum, adres en telefoonnummer.
Let op: De vrijstelling geldt alléén voor de meldingsplicht en betekent dus **niet** dat de wettelijke bepalingen uit de Wbp niet van toepassing zijn!

Wel of geen meldingsplicht?
Op de website van de Autoriteit Persoonsgegevens vindt u een handreiking bij het Vrijstellingsbesluit Wbp, welke helpt om te beoordelen of een verwerking van persoonsgegevens is vrijgesteld van de wettelijke meldingsplicht. Er kan geen algemeen antwoord worden gegeven op de vraag of thuisadministratie onder het vrijstellingsbesluit valt. De Autoriteit Persoonsgegevens stelt dat de verantwoordelijke hierin zelf een afweging moet maken.

Meldplicht Datalekken

Op 1 januari 2016 is de Wet Meldplicht Datalekken in werking getreden. Bij een datalek gaat het om onbedoelde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens. Onder een datalek valt dus niet alleen het vrijkomen van gegevens, zoals bij cyberaanvallen, gelekte computerbestanden of gestolen usb sticks of laptops, maar óók om onrechtmatige verwerking van gegevens.
Datalekken moeten, als ze ernstig genoeg zijn, binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens[5]. Als het waarschijnlijk is dat het lek ongunstige gevolgen zal hebben voor de betrokken personen, moeten zij hierover op de hoogte worden gebracht.

2. Beveiliging van persoonsgegevens

Volgens de Wbp moet de organisatie passende technische én organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Er zijn richtsnoeren opgesteld voor de beveiliging van persoonsgegevens, waarmee verbinding wordt gelegd tussen de wettelijke eisen van de Wbp en het domein van informatiebeveiliging (College Bescherming Persoonsgegevens, 2013). Uitgangspunt is dat al voorafgaand aan het verzamelen of verwerken van persoonsgegevens moet worden nagedacht over de risico's en de wijze van beveiliging. Ook moet de beveiliging van persoonsgegevens een continu aandachtspunt zijn in de organisatie, tot en met het wissen van het laatste backupbestand na afloop van de bewaartermijn. Er moet voortdurend gecontroleerd en geëvalueerd worden of de beveiliging nog adequaat is en/of moet worden aangepast.

2.1 Risicoanalyse

De verantwoordelijke inventariseert de dreigingen die kunnen leiden tot een beveiligingsincident, de

[4] Zie Artikel 3 Vrijstellingsbesluit Wbp.
[5] Het is aan een organisatie zelf om te beoordelen of een datalek ernstig genoeg is. De Autoriteit Persoonsgegevens heeft 'beleidsregels meldplicht datalekken' opgesteld, om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden.

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

gevolgen die dit incident kan hebben en de kans dat deze gevolgen zich voordoen. Bij verwerking via internet is hacking bijvoorbeeld een risico; bij verwerking op laptops of USB sticks is er risico op vermissing en diefstal. Er kunnen kwetsbaarheden of risico's aanwezig zijn in:
- *De beveiliging zelf:* bijvoorbeeld dat de vrijwilliger de gegevens onvoldoende beveiligt, of onzorgvuldig is in het verwerken of rapporteren. Ook kan het apparaat waarmee de gegevens worden verwerkt of opgeslagen onvoldoende beveiligd zijn.
- *Transparantie:* de verantwoordelijke moet kunnen vaststellen of de overeengekomen beveiligingsmaatregelen daadwerkelijk zijn getroffen. Ook moeten zowel de vrijwilligers als betaalde krachten eventuele beveiligingsincidenten tijdig en adequaat melden bij hun leidinggevende(n).
- *Continuïteit en overdraagbaarheid:* als de vrijwilliger stopt bij thuisadministratie, kan dit in bepaalde gevallen tot gevolg hebben dat gegevens over de hulpvrager, die wellicht een nieuwe vrijwilliger krijgt toegewezen, niet meer toegankelijk zijn voor de coördinator. Maak dus goede afspraken om dit te voorkomen. Dit geldt ook bij vertrek van een coördinator.

Verlies of onrechtmatige verwerking van persoonsgegevens kunnen meer of minder ernstige gevolgen hebben voor de betrokkenen. In de risicoanalyse kan onderscheid gemaakt worden tussen verschillende risicocategorieën. De gevolgen kunnen bijvoorbeeld ernstig zijn bij:
• Bijzondere persoonsgegevens (zie artikel 16 Wbp)
• Gegevens over de financiële of economische situatie van de betrokkene
• (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
• Gegevens die betrekking hebben op mensen uit kwetsbare groepen
• Gebruikersnamen, wachtwoorden en andere inloggegevens
• Gegevens die kunnen worden misbruikt voor (identiteits)fraude (CBP, 2013, p.19)

2.2 Het treffen van beveiligingsmaatregelen

Op basis van de risicoanalyse moeten passende beveiligingsmaatregelen worden getroffen, rekening houdend met de stand van de techniek en met de kosten om deze uit te voeren. Zie bijlage 1 voor een overzicht van gebruikelijke beveiligingsmaatregelen.

In de richtsnoeren die opgesteld zijn door het College Bescherming Persoonsgegevens (de oude naam van de Autoriteit Persoonsgegevens) wordt aangeraden om maatregelen te treffen op basis van algemeen geaccepteerde beveiligingsstandaarden die binnnen de informatiebeveiliging bestaan.[6] Zulke standaarden zijn gebaseerd op ervaringen en 'lessons learned' uit de dagelijkse praktijk. Er worden dan ook regelmatig nieuwe beveiligingsstandaarden en nieuwe versies gepubliceerd, die aansluiten op de nieuwste ontwikkelingen.

Organisaties moeten zowel technische als organisatorische maatregelen nemen. Dit houdt in dat organisaties moderne techniek moeten gebruiken om persoonsgegevens te beveiligen, maar ook binnen de organisatie duidelijk moeten afspreken wie toegang heeft tot welke gegevens. Er kunnen gedragsregels worden opgesteld, bijvoorbeeld hoe wordt omgegaan met het printen en kopiëren van gegevens.

Wat is een passend beveiligingsniveau?
Daarover moet de verantwoordelijke op basis van de risicoanalyse zelf een afweging maken. Het verschilt per context wat passende beveiligingsmaatregelen zijn.
Met de zich ontwikkelende techniek zal bovendien regelmatig een nieuwe afweging moeten worden gemaakt. In ieder geval moeten zowel organisatorische als technische maatregelen worden genomen. Focus bij het kiezen van maatregelen op het voorkómen van onnodige verzameling en verwerking van persoonsgegevens.

Er wordt aangeraden maatregelen te treffen op basis van algemeen geaccepteerde beveiligingsstandaarden (zie bijlage 1).
Zorg ook dat de gekozen maatregelen onderdeel zijn van de dagelijkse praktijk. Documenteer en specificeer ze in relevante documenten, zoals in werkinstructies of overeenkomsten. Evalueer met regelmaat of de maatregelen nog voldoende zijn.

[6] De Code voor Informatiebeveiliging is een zeer veel gebruikte beveiligingsstandaard, die binnen de informatiebeveiliging breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen. Er zijn ook specifieke standaarden voor specifieke sectoren, of voor specifieke toepassingen zoals webapplicaties.

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

Bewaartermijn van gegevens
Er wordt in de Wbp geen concrete bewaartermijn gesteld voor persoonsgegevens[7]. De wet bepaalt wel dat organisaties persoonsgegevens niet langer mogen bewaren dan nodig is voor het doel waarvoor ze zijn verzameld of gebruikt. Daarna moeten organisaties de gegevens zorgvuldig vernietigen[8].

2.3 Controle en evaluatie
De verantwoordelijke moet volgens de Wbp met regelmaat controleren of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Deze controle is extra belangrijk als de organisatie gebruikmaakt van een locatie die toegankelijk is voor publiek of die gedeeld wordt met andere organisaties.
De stand van de techniek en de kosten van de uitvoering van beveiligingsmaatregelen kunnen in de loop der tijd veranderen. Het totaal aan betrouwbaarheidseisen, maatregelen en controle wordt regelmatig geëvalueerd en waar nodig aangepast. Op deze manier kan een blijvend passend beveiligingsniveau worden bereikt.

3. Tips voor het beschermen van persoonsgegevens in thuisadministratie

De Wbp bepaalt dat organisatorische én technische maatregelen getroffen moeten worden om te voorkomen dat gegevens verloren raken of onrechtmatig worden verwerkt. Duidelijke afspraken maken met de vrijwilliger over wat hij/zij wel en niet mag doen is een organisatorische maatregel. Deze afspraken kunnen worden vastgelegd in de vrijwilligersovereenkomst. Bij de meeste diensten thuisadministratie is de insteek dat de hulpvrager in principe alles (zoals het invullen van gegevens op formulieren) zelf uitvoert, met ondersteuning en begeleiding van de vrijwilliger. Als de vrijwilliger dingen vóór de hulpvrager doet, is het risico groter dat gegevens verloren raken of onrechtmatig worden verwerkt. In dat geval zullen dan ook meer of zwaardere maatregelen moeten worden genomen om tot een passend beveiligingsniveau te komen.

Een aantal tips:

- De hulpvrager moet toestemming geven voor het verwerken van zijn/haar persoonsgegevens. Hij/zij moet snappen waarom bepaalde gegevens nodig zijn om de ondersteuning te kunnen uitoefenen. Informeer de hulpvrager al tijdens het eerste contact over wat de thuisadministratievrijwilliger wel en niet doet. Leg daarbij ook uit welke gegevens voor de vrijwilliger en/of de coördinator en/of de organisatie voor welke doelen noodzakelijk zijn om bij te houden of te delen (en met wie). Leg ook uit dat met de gegevens niet méér dan het noodzakelijke wordt gedaan, hoe lang ze worden bewaard en wat er gedaan wordt om onzorgvuldig gebruik van de gegevens te voorkomen.
- Persoonsgegevens mogen alleen voor welbepaalde en gerechtvaardigde doeleinden worden verzameld. Neem hierover een beschrijving op in het beleidsplan van de dienst thuisadministratie. Beschrijf ook de risico's, de beveiligingsmaatregelen en hoe de verantwoordelijkheden m.b.t. beveiliging van persoonsgegevens zijn verdeeld.
- Verzamel en gebruik niet méér persoonsgegevens dan nodig. Verwijder, waar mogelijk, namen en andere identificerende kenmerken uit de gegevens die worden verwerkt.
- Neem in de vrijwilligersovereenkomst duidelijke afspraken op over wat de vrijwilliger wel/niet mag doen met welke gegevens over de hulpvrager en wat te doen met de gegevens wanneer hij/zij stopt met het vrijwilligerswerk. Neem in de overeenkomst ook de verplichting tot geheim-houding op en wat de vrijwilliger zelf moet doen om het lekken van persoonsgegevens te

[7] In het vrijstellingsbesluit voor de meldingsplicht Wbp staat wel dat de persoonsgegevens uiterlijk twee jaar nadat de betrokkene te kennen heeft gegeven niet langer als begunstiger wil worden beschouwd, moeten worden verwijderd.
[8] Gegevens mogen langer worden bewaard voor historische, statistische of wetenschappelijke doelstellingen, mits er voorzieningen worden getroffen om te verzekeren dat de gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

voorkomen. Beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen moeten meteen gerapporteerd worden aan de coördinator.

- Maak van het beschermen van persoonsgegevens een onderwerp dat om de zoveel tijd besproken en geëvalueerd wordt tijdens groepsbijeenkomsten met vrijwilligers. Hiermee creëer je bewustzijn, transparantie en kunnen (nieuwe) knelpunten en risico's worden beoordeeld aan de hand van de praktijk.
- Beperk de toegang tot persoonsgegevens: hoe meer personen toegang hebben tot de gegevens, hoe groter de kans op misbruik.
- Rapporteren de vrijwilligers per e-mail aan de coördinator? Zorg dat de (Word/ Excel) bestanden waarin gegevens over de hulpvrager staan, beveiligd zijn met een wachtwoord.
- Loggen de vrijwilligers voor het rapporteren in op de website? Draag zorg voor een adequate toegangsbeveiliging van de website, alsook voor een afdoende bescherming van persoonsgegevens voor verdere verwerking door zoekmachines.
- Investeer in moderne beveiligingstechniek om te voorkomen dat gegevens gehackt kunnen worden.
- Voor beveiligingstechnologie is geld nodig. Maak de noodzaak hiervan duidelijk naar uw financiers! Volgens de richtlijnen van het College Bescherming Persoonsgegevens moet van verwerking van persoonsgegevens worden afgezien indien het realiseren van het vereiste beveiligingsniveau niet mogelijk is.
- Evalueer regelmatig of de gekozen organisatorische en technische beveiligingsmaatregelen nog afdoende zijn.

Uit de praktijk: hulpvrager heeft geen internet
Een regelmatig voorkomend dilemma bij thuisadministratie: de hulpvrager heeft thuis geen internet. En om bijvoorbeeld online formulieren in te vullen of in te loggen op DigiD is internet nodig. Om (al dan niet opzettelijk) onrechtmatig gebruik van de gegevens te voorkomen, is het onwenselijk dat vrijwilligers de gegevens (en al helemaal geen wachtwoorden) mee naar huis nemen. Het is beter om af te spreken dat de vrijwilliger samen met de hulpvrager naar een plek gaat waar computer en internet beschikbaar zijn, en waar de hulpvrager dus zelf de benodigde online handelingen doet of formulieren invult. Zij kunnen samen naar een openbare bibliotheek gaan, of gebruik maken van een computer die beschikbaar is op de locatie van de dienst thuisadministratie. Dit laatste heeft het voordeel dat de coördinator beter zicht heeft op het naleven van gedragsregels en dat eventuele kopieën bijvoorbeeld minder snel in onbedoelde handen kunnen vallen.
Heeft de hulpvrager wel internet, maar geen computer? Het gebeurt dat vrijwilligers zelf een laptop mee nemen naar de hulpvrager, om de financiële administratie digitaal te ordenen en/of online zaken te kunnen regelen met de hulpvrager. Het is veiliger om hiervoor een (leen)laptop van de dienst thuisadministratie te laten gebruiken, die de vrijwilliger niet voor andere doeleinden gebruikt. Na afloop van de ondersteuning of wanneer de 'relatie' door/met de vrijwilliger wordt beëindigd, wordt de laptop terug gegeven; de vrijwilliger beschikt dan niet langer dan nodig is over de gegevens.

4. Bronnen

- www.autoriteitpersoonsgegevens.nl
- College Bescherming Peroonsgegevens (2012). Richtsnoeren identificatie en verificatie van persoonsgegevens
- College Bescherming Peroonsgegevens (2013) Richtsnoeren beveiliging van persoonsgegevens
- www.justitia.nl/privacy
- Vrijstellingsbesluit Wbp
- Wet Bescherming Persoonsgegevens

Dit infosheet is tot stand gekomen mede dankzij mevr. Annie Korstjaans, coördinator Papierkroam bij Sythnese te Venray en dankzij mevr. Ria Steentjes, coördinator Op Ko€rs, Stichting Welzijn Hattem en Formulierenteam, SWO/E Welzijn & Ondersteuning Epe

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

Bijlage 1. Overzicht van gangbare beveiligingsmaatregelen

Bij het beoordelen van de beveiliging van persoonsgegevens wordt door de Autoriteit Persoonsgegevens uitgegaan van beveiligingsmaatregelen die binnen het vakgebied informatiebeveiliging gebruikelijk en vaak noodzakelijk zijn.
De volgende maatregelen worden genoemd in de richtsnoeren die door het College Bescherming Peroonsgegevens zijn opgesteld (2013, pp. 22-25):

• *Beleidsdocument voor informatiebeveiliging*
Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.

• *Toewijzen van verantwoordelijkheden voor informatiebeveiliging*
Alle verantwoordelijkheden zijn duidelijk gedefinieerd en verdeeld.

• *Beveiligingsbewustzijn*
Alle werknemers van de organisatie en -voor zover van toepassing- ingehuurd personeel en externe gebruikers krijgen, voor zover relevenat voor hun functie, training en regelmatige bijscholing over het informatiebeveiligingsbeleid en bijbehorende procedures van de organisatie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens.

• *Fysieke beveiliging en beveiliging van apparatuur*
IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.

• *Toegangsbeveiliging*
Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatie-systemen te voorkomen.

• *Logging en controle*
Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.

• *Correcte verwerking in toepassingssystemen*
In alle toepassingssystemen zijn beveiligingsmaatregelen ingebouwd.

• *Beheer van technische kwetsbaarheden*
Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden.

• *Incidentenbeheer*
Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd.

• *Afhandeling van datalekken en beveiligingsincidenten*
De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder. Als er aanleiding voor is, informeert hij ook de betrokkenen over het beveiligings-incident of het datalek.

• *Continuïteitsbeheer*
Door natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen kunnen persoons-

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl

gegevens verloren gaan. Door in de organisatie continuïteitsbeheer in te richten worden de gevolgen tot een aanvaardbaar niveau beperkt, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen.

• *Gegevensbescherming en geheimhouding van persoonsgegevens*
De organisatie heeft beleid ontwikkeld voor de bescherming en voor de geheimhouding van persoonsgegevens. Dit beleid is vastgelegd en geïmplementeerd en de organisatie communiceert dit naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens.

• *Geheimhoudingsovereenkomsten*
De verplichting tot geheimhouding van persoonsgegevens is vastgelegd in geheimhoudingsovereenkomsten.

In de informatiebeveiliging worden steeds meer ***privacy enhancing technologies*** (pet) gebruikt, technieken om de risico's voor de betrokkenen te beperken. Een centraal principe hierbij is het verminderen van de herleidbaarheid van de gegevens tot de betrokkenen. Denk bijvoorbeeld aan de automatische anonimisering van de verwerkte persoonsgegevens of aan het scheiden van (beveiligde) identificerende en niet-identificerende gegevens. Gangbare pet maatregelen zijn:

• *Encryptie (versleuteling) en hashing*
Encryptie (versleuteling) wordt toegepast bij verzending van persoonsgegevens via het internet, bij de opslag van persoonsgegevens op draagbare apparatuur en op verwijderbare media zoals usbsticks. Bij de opslag en verwerking van wachtwoorden wordt gebruik gemaakt van hashing (het omzetten van gegevens in een unieke code)[9].

• *Omgang met e-waste (afgedankte apparatuur en opslagmedia)*
Alle apparatuur die opslagmedia bevat, zoals laptops of smartphones, wordt ontdaan van de nog eventueel aanwezige persoonsgegevens alvorens het apparaat te verwijderen of hergebruiken. Apparatuur of opslagmedia met (gevoelige) persoonsgegevens worden fysiek vernietigd of het wordt onmogelijk gemaakt om de oorspronkelijke persoonsgegevens terug te halen, alvorens deze te verwijderen of hergebruiken.

[9] Cryptografiche bewerkingen zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Het is dus belangrijk om een goed ingericht sleutelbeheer te hebben. Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografiche bewerking die in de huidige situatie veilig genoeg is dat over een aantal jaren niet meer is.

LANDELIJK STIMULERINGSNETWERK THUISADMINISTRATIE ● Herengracht 220 ● 1016 BT Amsterdam ●
T 020 420 5945 ● F 020 638 2814 ● www.LSTA.nl ● thuisadministratie@maagdenhuis.nl