Handboek AVG Stichting Steenbreek

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

Samenvatting van de directie

De AVG-wetgeving is van toepassing op de activiteiten van Stichting Steenbreek: Stichting Steenbreek maakt gebruik van 'persoonsgegevens' (art. 2 ,3 en 4 AVG).

De juiste interpretatie van de AVG is nog gaande. De wet kent enige "onduidelijkheden". Stichting Steenbreek zal dan ook rekening moeten houden met toekomstige aanpassingen n.a.v. aanvullende richtlijnen vanuit de Autoriteit Persoonsgegevens. Stichting Steenbreek volgt in dit kader ook de aanvullingen in de Uitvoeringswet Algemene verordening gegevensbescherming [1]

Het handboek is niet in beton gegoten. Onze organisatie is een lerende organisatie. Er zullen nog fouten (incidenten) gaan voorkomen en naar aanleiding daarvan kunnen maatregelen (beschreven in dit handboek) worden bijgesteld.

Dit Handboek is bedoeld voor de drie bij de AVG betrokken partijen:

1. De Autoriteit Persoonsgegevens, die het recht heeft om bij ons te verifiëren of het beleid en doorgevoerde maatregelen voldoet aan de AVG
2. De medewerkers van Stichting Steenbreek: als communicatiemiddel zodat zij bewust worden van de consequenties van deze nieuwe wet,
3. Onze (ICT-)leveranciers. Wij kunnen aan de hand van dit handboek met hen afstemmen of de verwerking voldoet aan de regels van dit handboek.

[1] UAVG, zie: https://wetten.overheid.nl/BWBR0040940/2018-05-25

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

Inhoudsopgave

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

1 Het AVG-beleid bij Stichting Steenbreek

Het AVG-beleid bij Stichting Steenbreek is uitgewerkt in een aantal onderwerpen. Alle onderwerpen zijn van gelijkelijk belang voor het uiteindelijke resultaat: de verwerking van persoonsgegevens afdoende gewaarborgd, naar de regels van de AVG.

1.1 Beleid m.b.t. de doelbinding en grondslagen verwerking

Doelstellingen van Stichting Steenbreek

Stichting Steenbreek is een kennis- en netwerkorganisatie met een missie om onze leefomgeving in Nederland te vergroenen in het kader van klimaatadaptatie, biodiversiteit, sociale cohesie en gezondheid. Stichting Steenbreek werkt met aangesloten gemeenten en partners en organiseert communitys binnen haar kernthema's. Daarvoor is onder meer verwerking van persoonsgegevens noodzakelijk.

Beleid

Het beleid van Stichting Steenbreek is erop gebaseerd dat uitsluitend persoonsgegevens worden verwerkt noodzakelijk voor de ondersteuning van de bedrijfsprocessen voor het realiseren van haar doelstelling.

Beleid m.b.t. de grondslagen voor verwerking

Voor het gerechtvaardigd zijn van een verwerking is een grondslag nodig naar de eisen van art. 6 AVG. Er zijn diverse grondslagen, waarvan er voor Stichting Steenbreek maar enkele relevant zijn:

1. wettelijke verplichting, b.v. info te verstrekken aan belastingdienst
2. overeenkomst, b.v. verkoopcontracten met klanten en arbeidscontracten werknemers
3. uit gerechtvaardigd belang, deze grondslag moet voldoen aan de duidelijke criteria van 'welbepaaldheid' en uitdrukkelijk omschreven zijn
4. met toestemming van betrokkenen

Register van Verwerkingen

Voor de details m.b.t. de systemen, administraties, grondslagen e.d. zie het Register van Verwerkingen.

1.2 Beleid m.b.t. Verwerkersovereenkomsten

Met iedere Verwerker die voor Stichting Steenbreek persoonsgegevens (van de administraties als in de registers) verwerkt, moet de Verwerkingsverantwoordelijke een verwerkersovereenkomst aangaan.

Het beleid is erop gericht om het initiatief bij de Verwerker te laten liggen om tot een Verwerkersovereenkomst te komen. Dit is natuurlijk om praktische redenen: de Verwerker heeft (meestal) meerdere klanten voor wie mijn of meer dezelfde overeenkomst gemaakt moet worden.

Als een Verwerker geen Verwerkersovereenkomst heeft en ook niet binnen enige maanden zal aanleveren, dan zal de Verwerkingsverantwoordelijke het Model Verwerkersovereenkomst aanbieden zie bijlage

De volgende situaties doen zich voor:

1. Een getekende Verwerkersovereenkomst. De Verwerkingsverantwoordelijke en Verwerker sluiten gezamenlijk een Verwerkersovereenkomst die voldoet aan de AVG voorzien van handtekeningen

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

2. Een verwerkersovereenkomst van een Grote Organisatie. De Verwerker is een groot bedrijf (zoals Google, Microsoft, Mailchimp etc.), met zo'n soort bedrijf kan vaak geen individuele overeenkomst worden afgesloten. De Verwerkingsverantwoordelijke laat c.q. gaat alle juridische stukken onderzoeken om te bepalen of voldaan wordt aan de AVG:

a. Indien dit het geval is, dan zal de Verwerkingsverantwoordelijke periodiek (in de praktijk is de afspraak dat de betrokken collega verantwoordelijk is voor de jaarlijkse evaluatie) onderzoeken of er niks gewijzigd is in de juridische stukken van de Verwerker

b. Indien dit niet het geval is, dan zal Stichting Steenbreek een andere Verwerker gaan zoeken.

1.3 Beleid m.b.t. minimale gegevensverwerking

Er zullen niet meer gegevens worden verzameld dan die welke voor het verwerken van een administratie noodzakelijk zijn ('genoeg is genoeg'). Per administratie zullen de te verwerken gegevens worden vastgesteld.

1.4 Beleid m.b.t. het verzamelen van gegevens

Voor het verwerken van persoonsgegevens uit de administraties zullen gegevens worden verzameld. In de Bijlage 1 wordt bij iedere administratie vastgelegd wat de herkomst is van alle privacygevoelige gegevens zijn.

Gegevens van personen zullen alleen worden gebruikt:

1. indien de Betrokkenen expliciet toestemming hebben verleend. De toestemming moet kunnen worden aangetoond.
2. indien de Persoonsgegevens afkomstig zijn van publieke bronnen (o.a. van sociale media).
3. indien de Persoonsgegevens afkomstig zijn van een aangekocht en "legitiem" databestand. Stichting Steenbreek dient wel te onderzoeken en vast te stellen of een leverancier zich gehouden heeft aan de eisen van de AVG.

1.5 Beleid m.b.t. Direct Marketing

Stichting Steenbreek organiseert inspirerende bijeenkomsten en probeert betrokkenen middels kruisbestuiving te verbinden. Rode draad hierin zijn onderwerpen binnen het domein waar Stichting Steenbreek opereert: vergroening.

Nieuwe campagnes dienen vooraf door de directie te worden goedgekeurd.

Voor communicatie met Betrokkenen in het kader van DM is het opnemen van die gegevens in een mailingbestand noodzakelijk. Er bestaat bij DM (doorgaans) geen contractuele relatie met de Betrokkene; zij zijn (functioneel) breed geïnteresseerd in de diensten en de informatie van Stichting Steenbreek. Een mailing aan Betrokkene wordt daarom geacht op grondslag van *gerechtvaardigd belang* te worden gedaan.

Betrokkenen in bestanden van Stichting Steenbreek hebben voor het opnemen daarin direct of indirect voor toepassing van DM-mailings hun toestemming gegeven. Toestemming voor opname in het emailing-bestand wordt aangenomen te zijn, als:

1. Betrokkene zich, op wat voor manier dan ook, voor de mailings opgeeft. De gebruikelijke manier is het aanvinken van de optie 'toezenden mailing' op de site of via de link in een proef-mailing.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

2. Betrokkene zijn gegevens aan Stichting Steenbreek of een vertegenwoordiger van Stichting Steenbreek verstrekt. Ook het afgeven van een visitekaartje valt hieronder.
3. Betrokkene duidelijk blijk heeft gegeven van een functionele of zakelijke relatie met de diensten van Stichting Steenbreek.
4. Betrokkene gedurende langere tijd (tenminste 3 keer) al deel uitmaakt van de mailings via de mailinglist en zich niet door middel van de opt-out, die iedere mailing biedt, heeft uitgeschreven.
5. Betrokkene een zodanige functie heeft dat die als publiekelijk of publiekelijk bekend mag worden beschouwd.
6. Informatie van en over Betrokkene bekend is gemaakt via openbare publicaties, o.a. de sociale media.

Van actieve aanmeldingen voor DM en van overeenkomsten met Betrokkenen wordt aantekening gehouden in de applicatie "Mailcamp".

1.6 Beleid m.b.t. de verwerking voor andere doeleinden

Het is de Verwerkingsverantwoordelijke en Verwerker niet toegestaan de gegevens voor een ander doel te verwerken dan aangegeven als in § 1.1 Beleid m.b.t. Doelbinding en in §1.2 Beleid m.b.t. Grondslagen van dit Handboek.

Indien een voornemen voor verwerking voor andere doeleinden dan in de administraties gedefinieerd zich voordoet, zal daaraan een MT-beslissing ten grondslag moeten liggen. De Verwerkingsverantwoordelijke wordt dan via een aanwijzing geïnstrueerd. De administraties en registers worden bijgewerkt alvorens een andere verwerking uit te voeren.

1.7 Beleid m.b.t. verwerken van bijzondere categorieën

Stichting Steenbreek registreert en verwerkt geen bijzondere categorieën van gegevens als in art. 9 van de AVG. Stichting Steenbreek registreert en verwerkt geen gegevens betreffende strafrechtelijke veroordelingen en/of strafbare feiten. Het is verboden gegevens onder die categorieën op enigerlei wijze te verzamelen en/of te verwerken.

1.8 Beleid m.b.t. personen jonger dan 16 jaar

Het controleren en verkrijgen van toestemming voor verwerking van persoonsgegevens van kinderen is door de aard van de activiteiten van Stichting Steenbreek niet van toepassing. Indien zich zo'n situatie mocht (of lijkt) voordoen zal Stichting Steenbreek nagaan of dat de bedoeling is geweest, met inachtneming van het gestelde in art. 8 van de AVG.

1.9 Beleid m.b.t. doorgifte van gegevens

Doorgifte van gegevens aan landen buiten de EU en/of Internationale Organisaties is niet toegestaan, tenzij wettelijk verplicht

1.10 Beleid m.b.t. geautomatiseerde verwerking

Bij Stichting Steenbreek vindt geen geautomatiseerde (individuele) besluitvorming of profilering plaats op basis van de gegevens uit de administraties.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

1.11 Beleid m.b.t. archivering

Archivering van gegevens vindt plaats naar aard en relevantie van de administraties, in de Register (zie bijlage 1) wordt dit nader gespecificeerd.

1.12 Beleid m.b.t. de koppelingen met andere systemen

Het beleid is om in principe geen koppelingen met andere systemen aan te leggen. Als dit echt nodig is dan wordt in de registers van bijlage 1 expliciet vastgelegd wat de reden is van deze koppeling. De volgende mogelijkheden zijn er:

1. Informatie wordt uit een ander systeem (van een andere organisatie) gehaald en vastgelegd in de eigen toepassing.
2. Informatie wordt uit een ander systeem geraadpleegd tijdens de verwerking maar niet vastgelegd in de eigen toepassing.
3. Informatie wordt ingebracht in een ander systeem (doorgifte).
4. Het andere systeem kan informatie raadplegen.

1.13 Beleid m.b.t. pseudonimisering bij analyses

Het beleid is dat het verwerken van persoonsgegevens op zodanige wijze wordt uitgevoerd zodat de persoonsgegevens niet meer aan een specifieke Betrokkene kunnen worden gekoppeld.

Ten behoeve van analyses voor (strategisch) bedrijfsbelang kunnen gegevens van alle administraties worden gebruikt, mits deze gepseudonimiseerd conform bovenstaande tekst.

Voor Stichting Steenbreek is deze paragraaf niet van toepassing

1.14 Beleid m.b.t. het omgaan met inbreuken

Geconstateerde inbreuken worden afgehandeld conform art. 33 van de AVG. Van constateringen, afhandeling en resultaat wordt aantekening gehouden zie verder 2.2.2 Proces: Acteren op inbreuken | Ref: AVG art. 33

1.15 Beleid m.b.t. een FG [2]

Stichting Steenbreek kent op grond van de eisen gesteld in art. 37 van de AVG geen specifieke positie van Functionaris voor de Gegevensbescherming toe.

Er zal geen Functionaris voor de Gegevensbescherming worden aangesteld; de directie is collegiaal verantwoordelijk voor de gegevensbescherming.

[2] FG = Functionaris voor de Gegevensbescherming

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

1.16 Beleid m.b.t. de beveiliging en toegang tot de informatie

Voor de beveiliging van en de toegang tot informatie zijn organisatorische en technische maatregelen getroffen:

1. De organisatorische maatregelen zijn beschreven in hoofdstuk 2.
2. Voor de technische maatregelen, zie hoofdstuk 3. Stichting Steenbreek heeft ervoor gekozen om enige artikelen uit de ISO 27001 te implementeren.

1.17 Beleid m.b.t. Personeel

Het beleid m.b.t. het eigen Personeel:

1. er wordt regelmatig getoetst of medewerkers hun verantwoordelijkheden begrijpen en derhalve geschikt zijn voor het uitvoeren van hun functie,
2. medewerkers worden dit handboek ter beschikking gesteld.

In de arbeidsovereenkomst wordt de clausule opgenomen:

a. dat de medewerker dit handboek heeft ontvangen,
b. dat de medewerker is verplicht tot geheimhouding van alle gegevens over het bedrijf, de bedrijfsvoering en klanten van de werkgever waarvan hij weet of redelijkerwijze kan vermoeden dat deze vertrouwelijk zijn.
c. Deze verplichting geldt ook na beëindiging van de arbeidsovereenkomst.
d. Bij ondertekening van deze arbeidsovereenkomst gaat de medewerker akkoord met deze geheimhoudingsverplichting,
e. De geheimhoudingsovereenkomst wordt afgesloten voordat persoonsgegevens (mogen) worden verwerkt

3. Alle medewerkers krijgen een bewustzijnstraining en zullen regelmatig worden bijgeschoold (eerstkomende keer: juni 2021).
4. Het beleid m.b.t. Personeel van de Verwerker geldt dat er min of meer dezelfde regels van toepassing zijn als voor de eigen medewerkers. Dit wordt vastgelegd in de verwerkersovereenkomst.

1.18 Beleid m.b.t. Gegevensbescherminsgeffectbeoordeling

De grootte en de aard van de gegevens bij Stichting Steenbreek verplichten niet tot het uitvoeren van een gegevensbeschermingseffectbeoordeling.
Stichting Steenbreek heeft met dit handboek een beleid opgesteld dat, naar haar mening, voldoet aan de door de AVG gestelde passende organisatorische en technische maatregelen.

1.19 Beleid m.b.t. risico' s op inbreuk

Het risico op inbreuk op de gegevens bij Stichting Steenbreek wordt niet hoog ingeschat. Voor het voorkomen van inbreuken zijn technische en organisatorische maatregelen genomen naar de stand van de techniek, in overeenstemming met de eisen van de AVG. Technische maatregelen zijn verwoord in hoofdstuk 3 van dit handboek.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

1.20 Beleid m.b.t. bezwaar, beperken en wissen

Indien Betrokkene verzoekt te worden gewist, beperkt wil worden in verwerking of bezwaar maakt tegen verwerking, moet dat in principe worden gehonoreerd.

Er kunnen omstandigheden zijn waarin het een vitaal belang van Betrokkene of van anderen is om het verzoek niet te honoreren of dat Stichting Steenbreek zelf prevalerende dwingende gerechtvaardigde gronden heeft voor de verwerking. In dat geval mag Stichting Steenbreek een aantal maatregelen nemen:

- persoonsgegevens alsnog verwerken of
- persoonsgegevens niet (direct) wissen

Voor beleid van bezwaar wordt het beleid van wissen en beperken aangehouden.

1.20.1 Beleid in het geval van wissen en beperken

Stichting Steenbreek voert, op verzoek daartoe, de procedures op basis van hoofdstuk 3 van dit handboek, de nodige stappen uit om persoonsgegevens te wissen of in beperking te stellen.

Voor het wissen worden, rekening houdend met de beschikbare technologie en met de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, genomen.

In het geval van beperking van verwerking van die doeleinden, moet de Verwerkingsverantwoordelijke, bij het verzamelen van (nieuwe) gegevens toetsen en zeker stellen of daarin gegevens van Betrokkene voorkomen, om te voorkomen dat die worden verwerkt.

Het bestand waarin de “gewiste” persoonsgegevens worden bewaard, dient enkel dit doel en wordt verder strikt beperkt! Bij het beperken wordt zeker gesteld dat de kans op inbreuk door onrechtmatig verwerken van persoonsgegevens minimaal is.

Betrokkene wordt van de maatregelen en, zo mogelijk, van het resultaat op de hoogte gesteld.

1.20.2 Situaties waarin belangen van Betrokkene ondergeschikt zijn

Veel persoonsgegevens zijn geënt op digitale informatie waarin emailadressen een centrale vervullen. Indien Betrokkene zeker wil stellen dat verwerking na een verzoek daartoe niet meer plaatsvindt en ook niet meer zal plaatsvinden, zullen aanvullingen op een te verwerken bestand daarop moeten worden gecontroleerd.

Het beleid van Stichting Steenbreek is daarom dat voorafgaand aan iedere verwerking van persoonsgegevens waarop aanvullingen zijn gedaan sinds de beperking of het wissen, een controle wordt gedaan of de gegevens van Betrokkene niet op een of andere wijze alsnog zijn toegevoegd.

Stichting Steenbreek zal dan ook minimaal een bestand aanhouden dat email-adressen van Betrokkenen die verzocht hebben om beperkt te worden in verwerking of te worden geëist, aanhouden.

het bestand “beperkte” persoonsgegevens mag voor geen enkele andere doel worden gebruikt. Er is geen duur voor wissen van dat bestand vastgesteld.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

1.20.3 Grondslagen voor afwijkend beleid

De grondslagen voor het afwijken op verzoeken tot beperken of wissen zijn:

"art. 6.1.d: ...de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;..."

"art 17.1.c: ... wissen hoeft niet wanneer betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking,...;"

"art.21.: ...De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens (in het geval van bezwaar) tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene... ."

1.21 Beleid m.b.t. rapportages, controles en audits

Ten behoeve van de controle op het juiste en rechtmatige toepassing en het functioneren van de AVG en de organisatie zullen rapportages, controles en audits worden gedaan.

De Verwerkingsverantwoordelijke is verantwoordelijk voor het controleren op de juiste toepassing van het AVG-beleid en van de toepassing van de maatregelen van dit handboek. Hij stelt jaarlijks een controleschema op.

Audits kunnen worden gepland en uitgevoerd conform het interne kwaliteitsbeleid. Audits door de toezichthouder, vallen hier ook onder.

1.22 Beleid t.a.v. interne werkprocessen

Voor de uitvoering van de AVG binnen Stichting Steenbreek zijn interne werkprocessen vastgesteld en beschreven in Hoofdstuk 2.

De directie is proceseigenaar van de processen. De uitvoering van de processen is bindend. Toestemming voor afwijking daarvan kan alleen door de de directie worden gegeven.

1.23 Beleid m.b.t. mitigerende maatregelen

Mitigerende maatregelen kunnen worden genomen naar aanleiding van incidenten (soms direct), controles, audits en evaluaties.

De Verwerkingsverantwoordelijke is geautoriseerd tot het nemen van tijdelijke mitigerende maatregelen. De directie moet deze tijdelijke maatregelen verwerken in dit handboek opdat het definitieve maatregelen zijn geworden.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

2 AVG intern georganiseerd

2.1 Functies en Taken

2.1.1 Taken van de directie

De directie van Stichting Steenbreek is verantwoordelijk voor de invoering en de toepassing van het AVG-beleid en van de maatregelen beschreven in dit handboek.

De directie ziet er actief op toe dat het AVG-beleid wordt geïmplementeerd. Hij treft maatregelen indien wordt geconstateerd dat het handboek niet wordt toegepast of dat er anderszins lacunes zijn in het voldoen aan de AVG. De directie stelt de Verwerkingsverantwoordelijke en de Verwerker in staat het beleid adequaat uit te voeren.

2.1.2 Taken van de Verwerkingsverantwoordelijke

De Verwerkingsverantwoordelijke is verantwoordelijk voor het uitvoeren van de maatregelen van de AVG als beschreven in dit handboek.

De formele taken van de Verwerkingsverantwoordelijke zijn:

1. het uitvoeren van het beleid verwoord in dit handboek,
2. het maken van (schriftelijke instructies) voor de V's, in lijn met dit handboek,
3. bepalen welke eigen medewerkers toegang krijgen tot specifieke registers,
4. het zorgdragen voor het aangaan en uitvoeren van Verwerkers- overeenkomsten:

a. met iedere (ICT-) leverancier die persoonsgegevens verwerkt of daar toegang toe heeft,
b. bij grote leveranciers bij voorkeur een verwerkers- overeenkomst van hen,
c. dat speciale aandacht wordt besteed aan de afhankelijkheid van leveranciers van derde partijen. Dat geldt met name voor cloud (hosting) omgevingen die zij daarvan betrekken,

5. het regelmatig evalueren van het beleid,
6. het gevraagd en ongevraagd adviseren aan MT om beleid aan te passen,
7. het (laten) bijhouden van registers (bijlage 1),
8. het aannemen van verzoeken van Betrokkenen en het beleggen van deze verzoeken in de organisatie,
9. het assisteren bij inspecties,
10. het geven van toestemming aan de V's dat taken en bevoegdheden aan andere V' s kunnen worden gedelegeerd,
11. het zorgdragen voor voldoende competent personeel als het gaat om de kennis over de AVG en de toepassing hiervan.

De Verwerkingsverantwoordelijke zorgt ervoor dat personeel tenminste voldoet aan:

a. het hebben van kennis van de administraties die worden gevoerd,
b. het hebben van kennis van de Verwerkersovereenkomsten,
a. het hebben van kennis van de Applicaties waarmee administraties worden gevoerd.

2.1.3 Taken van de Verwerker | Ref: AVG art. 28.

De taken van de Verwerker zijn:

1. de Verwerker handelt in de geest van de AVG en van dit handboek

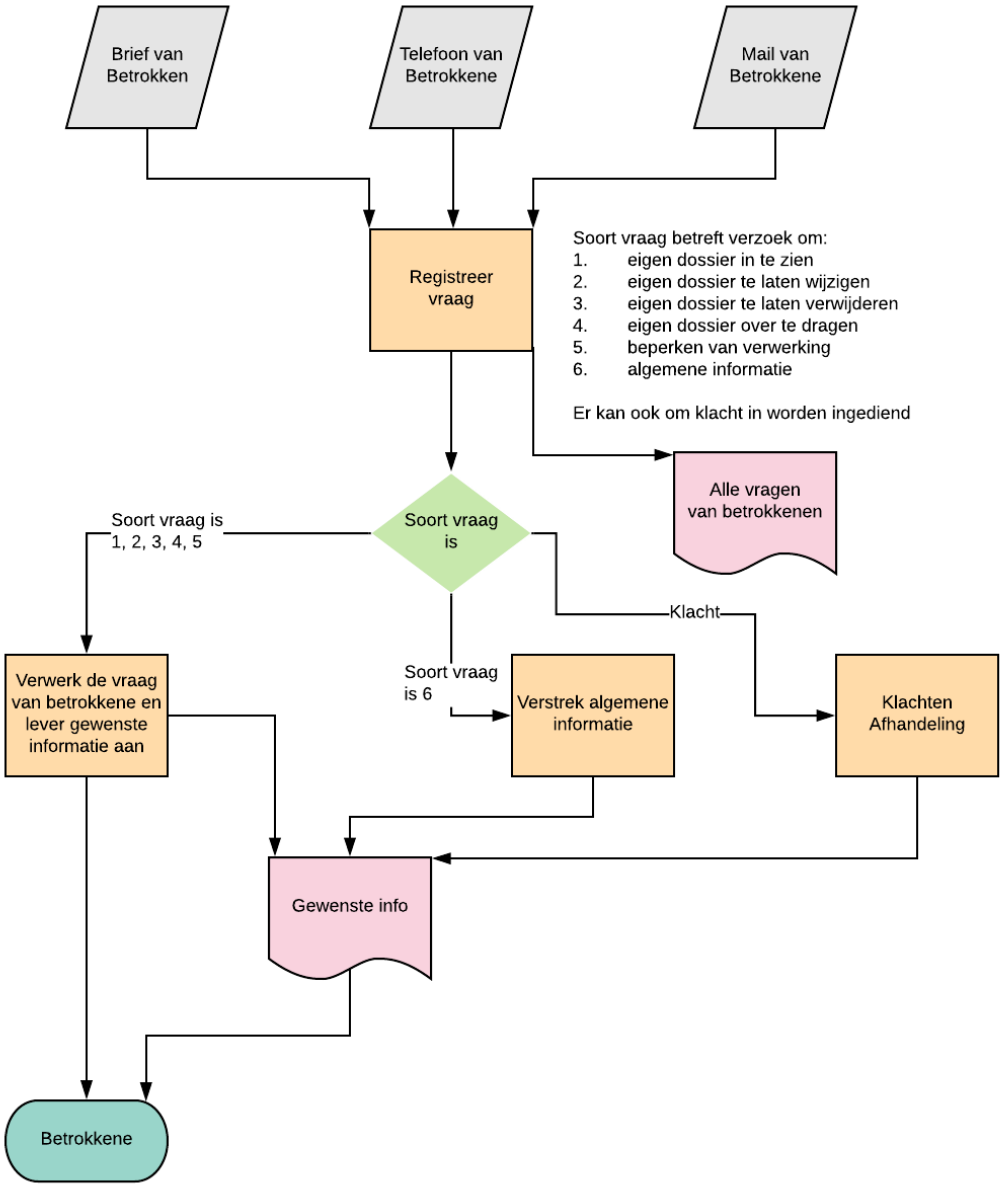
2. de Verwerker zal alleen Persoonsgegevens verwerken in opdracht van de Verwerker, de Verwerker heeft geen zeggenschap over de Persoonsgegevens,

3. de Verwerker zal volgt de instructies van de Verwerkingsverantwoordelijke, als in de verwerkersovereenkomst, op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij de Verwerkingsverantwoordelijke daar van te voren toestemming of opdracht voor geeft c.q. heeft gegeven.,

4. de Verwerker neemt geen andere verwerker (onderaannemer) in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de Verwerkingsverantwoordelijke.

2.2 Afhandelen van vragen van Betrokkenen

2.2.1 Proces



Alle

vragen van Betrokken en gegeven antwoorden worden vastgelegd in een register: zie 2.3.2 Registratieformulier-Vraagafhandeling. De processtappen worden onder verantwoordelijkheid van de Verwerkingsverantwoordelijke doorgevoerd.

Basis-processtappen:

1. verzoeken en vragen van Betrokkenen kunnen binnenkomen via mail, post of een telefoontje. Vragen worden bij de Verwerkingsverantwoordelijke ingediend,
2. de Verwerkingsverantwoordelijke registreert vragen en verzoeken op het Registratieformulier-Vraagafhandeling, hierop staat oa. de NAW van Betrokken, de Datum vraag en de soort vraag: bestaande uit:
   a. eigen dossier in te mogen zien,
   b. eigen dossier te laten wijzigen,
   c. eigen dossier te laten verwijderen,
   d. eigen dossier over te dragen,
   e. beperken van verwerking,
   f. algemene informatie,
   g. een klacht.
3. in het geval van situaties a t/m e wordt het gewenste verzoek procedureel doorgevoerd en Betrokkene worden geïnformeerd. Op het Registratieformulier-Vraagafhandeling zal de datum afgifte genoteerd worden.
4. in het geval van algemene informatie, beoordeelt de Verwerkingsverantwoordelijke of de gewenste algemene informatie verstrekt kan/mag worden.
   Op het Registratieformulier-Vraagafhandeling wordt de datum afgifte genoteerd . Indien de Betrokkene niet tevreden is omtrent de geleverde informatie wordt dit dossier omgezet in een klacht.
5. in het geval van een Klacht, zal de Verwerkingsverantwoordelijke contact opnemen met de DIR. Mogelijk wordt zelf de Privacy-jurist geraadpleegd om te bepalen of de klacht gegrond is. De DIR dan wel de Verwerkingsverantwoordelijke zal persoonlijk contact opnemen met degene die de klacht ingediend heeft.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

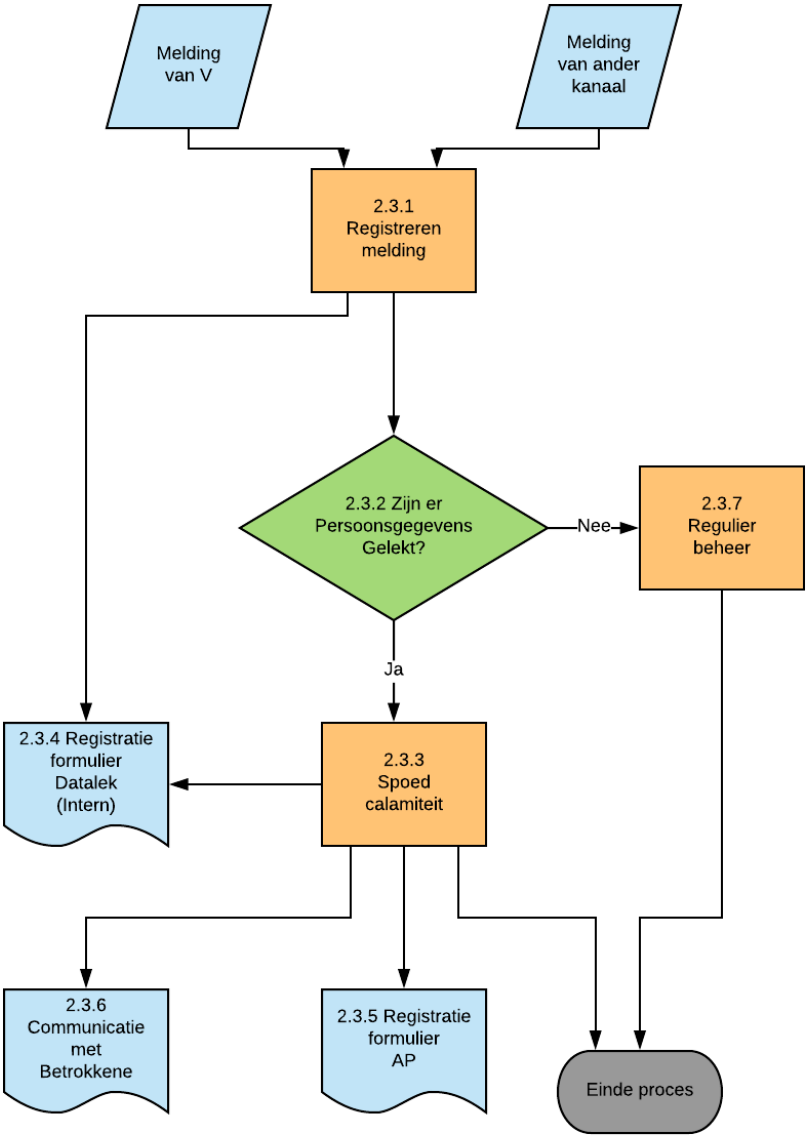
2.2.2 Registratieformulier-Vraagafhandeling

Iedere vraag, klacht etc. van een Betrokkene wordt in dit formulier vastgelegd, zie samenhangend proces: 2.2 Afhandelen vragen van Betrokkenen

Datum vraag	dd-mm-jj
Omschrijving vraag	
Soort vraag	Maak keuze uit: ❑ eigen dossier inzien ❑ eigen dossier wijzigen ❑ eigen dossier verwijderen ❑ eigen dossier over te dragen ❑ beperken van verwerking ❑ algemene informatie ❑ klacht ❑ anders
Naam, mail en GSM van betrokkene	
Opgepakt door (b.v. Verwerkingsverantwoordelijke of ICT-specialist)	
Beschrijving afhandeling	
Status	❑ nieuw ❑ mee bezig ❑ afgehandeld

2.3 Acteren op inbreuken (Datalek)

2.3.1 Registreren Melding



Bij paragraaf 2.3.4 staat de layout van het Registratieformulier Datalek (intern) . Dit formulier is een verkorte versie van het aanmeldingsformulier van de AP. Bij het Registeren van de melding wordt dit formulier al deels ingevuld.

Afkomst melding

Op het Registratieformulier Datalek (intern) staat aangegeven van wie de melding afkomstig is.

1. van de Verwerker,
2. via eigen constatering,

3. via een Audit of PenTest,
4. via een nieuwe ISO/NEN eis,
5. via wijziging in wet en regelgeving,
6. via leverancier van één van de vele software onderdelen die gebruikt worden in uw applicaties,
7. via ander kanaal.

2.3.2 Zijn er Persoonsgegevens gelekt?

(Vermeende) inbreuken op de privacy worden onmiddellijk door de Verwerker aan de Verwerkingsverantwoordelijke gemeld, ook als er nog niet duidelijk is of er sprake is van een datalek.

De Verwerker moet dit uiterlijk binnen 24 uur melden omdat de Verwerkingsverantwoordelijke de plicht heeft datalekken binnen 72 uur aan te melden (aan de AP).

Indien er (nog) geen persoonsgegevens gelekt zijn, maar hierop wel een risico bestaat, Ga dan verder met 2.3.6 Regulier beheer.

2.3.3 Spoed calamiteit

In de crisis-aanpak wordt een checklist afgewerkt van acties:

1. Belangrijk is dat de Verwerkingsverantwoordelijke en Verwerker ook in het weekend goed bereikbaar zijn. Afhankelijke van de omvang van de calamiteit kan er voor gekozen worden om een 24 uurs bezetting te creëren. De werktijden voor Verwerkingsverantwoordelijke en Verwerker zijn minimaal:
a. Ma. t/m Vr. van 9:00 tot 22:00
b. Zaterdag. van 9:00 tot 22:00
c. Zondag van 9:00 tot 22.00
2. indien zinvol (dit ter beoordeling door de V) zal de server (applicatie) tijdelijk off line gezet worden, bijv..om het lekken direct te laten stoppen.
3. de Verwerker zal direct starten met een onderzoeken wat de impact van een inbreuk is. De Verwerker zal ook de benodigde ICT experts alloceren.
4. In dit onderzoek worden de volgende aspecten meegenomen:
a. welke persoonsgegevens zijn gelekt?
b. hoeveel persoonsgegevens zijn gelekt?
c. wat is de oorzaak van het lek?
d. is er een tijdelijke “workaround” beschikbaar, opdat men zo snel mogelijk weer kan werken?
e. kan een eerste inschatting gemaakt worden hoe lang een oplossing gaat duren?
5. de Verwerkingsverantwoordelijke stelt De DIR direct op de hoogte van het incident. De DIR beoordeelt zelf of zij de afhandeling overlaat aan de Verwerkingsverantwoordelijke alleen,
6. de Verwerkingsverantwoordelijke stelt binnen 72 uur de Autoriteit Persoonsgegevens op de hoogte van het lek, *indien het daadwerkelijk een datalek blijkt te zijn en er risico op gevolgen voor Betrokkene zijn,*
7. de Verwerkingsverantwoordelijke stelt de getroffen Betrokkenen op de hoogte van het lek.

2.3.4 Registratieformulier Datalek (intern)

1	Datum tijd incident	dd-mm-jj hh:mm Dit betreft het tijdstip waarop de Verwerkingsverantwoordelijke op de

		hoogte is gesteld van het incident
2	Omschrijving melding	Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem
3	Afkomst melding	Maak keuze uit: ❑ van de V ❑ via eigen constatering ❑ via een Audit of PenTest ❑ via een nieuwe ISO/NEN eis ❑ via wijziging in wet en regelgeving ❑ via leverancier ❑ via ander kanaal
4	Zijn er persoonsgegevens gelekt?	❑ Spoed calamiteit ❑ Behandelen in regulier proces ❑ Weet niet
5	Aantal Betrokkenen	Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident? Geef a.u.b. een minimum en maximum aantal persone
6	Categorieën	Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?
7	Soort Betrokkene	Omschrijving groep personen om wiens gegevens het gaat. Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen
8	Betrokkenen bekend?	Zijn de contactgegevens van de betrokken personen bekend? Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken
9	Registers	Welke Registers (zie bijlage 1) zijn geraakt
10	Oorzaak	Wat is de oorzaak van het beveiligingsincident? Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan? Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? Geef dit a.u.b. zo specifiek mogelijk aa

11	Beschrijving afhandeling	
	Status	❑ nieuw ❑ mee bezig ❑ afgehandeld

2.3.5. Aanmeldingsformulier bij AP

Het aanmelden van een datalek: procedure: zie de site van de AP:
https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Bij Twijfel of de aanmelding nodig is: gewoon aanmelden!

2.3.6 Communicatie met betrokkenen

In principe worden alle betrokkenen op de hoogte gesteld van het lekken van hun persoonsgegevens, tenzij er een dringende reden bestaat om dit niet te doen, in dat geval zal de AP toetsen of de genoemde reden " dringend" is.

2.3.7 Regulier beheer

De meeste meldingen hebben geen spoed, maar dienen wel te leiden tot een onderzoek en analyse en wellicht nieuwe maatregelen. Afhandeling van dit soort meldingen is een standaard onderdeel van het reguliere technische ICT beheer.

De Verwerkingsverantwoordelijke hoeft niet structureel op de hoogte worden gebracht van alle zaken die in het regulier beheer zijn behandeld. Op verzoek kan de Verwerkingsverantwoordelijke eens per jaar om een rapportage vragen.

De Verwerker wordt wel dringend geadviseerd alle meldingen en doorgevoerde acties te registreren

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

3 Technische maatregelen

3.1 Register van Bedrijfsmiddelen

Alle bedrijfsmiddelen worden in een inventarisatie overzicht benoemd en vastgelegd. Per middel wordt geregistreerd:

1. nummer (ID) van het bedrijfsmiddel
2. naam medewerker die bedrijfsmiddel in bezit heeft
3. naam leverancier
4. geïnstalleerde software
5. beschrijving van doorgevoerde beveiligingsmaatregel(en), zie §3.2
6. garantietermijn (datum einde garantie)
7. laatste controle door ICT-specialist

3.2 Beveiligingsmaatregelen op bedrijfsmiddelen

Voor bedrijfsmiddelen gelden de volgende basisregels:

1. een bedrijfsmiddel is, waar mogelijk, zo ingericht dat er geen persoonsgegevens worden opgeslagen ('zero footprint')
2. voor het geval dat een zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, worden de in onderstaande paragrafen beschreven maatregelen doorgevoerd. Denk hierbij ook aan het feit dat er er niets direct gegevens opgeslagen behoeven te zijn, maar dat ook automatisch ingelogd kan worden in privacygevoelige systemen omdat user/paswoorden zijn opgeslagen op het Bedrijfsmiddel
3. alle in onderstaande paragrafen gestelde maatregelen worden doorgevoerd door de ICT-specialist, tenzij anders aangegeven.

3.2.1 Doorgevoerde beveiligingsmaatregelen m.b.t. Werkstations

Voor Werkstations gelden de volgende maatregelen:

1. Ieder Werkstation kan door één of meerdere gebruikers benut worden. Iedere gebruiker heeft een unieke user en password voor de toegang tot zijn eigen omgeving.
2. Ieder Werkstation zal na 15 minuten in de slaapstand gezet worden.
3. Ieder Werkstation wordt uitgerust met een virus-programma.
4. De harddisk van het Werkstation wordt encrypted.
5. Wanneer een Werkstation naar een reparateur gaat, zal ICT-specialist het Werkstation onderzoeken of er persoonsgegevens lokaal opgeslagen zijn:
   - indien JA:
     i. zal de ICT-specialist zal gebruiker vragen deze persoons- gegevens elders op te slaan of te verwijderen,
     ii. zal de ICT-specialist de persoonsgegevens verwijderen,

     alvorens het Werkstation naar de reparateur kan.
   - indien NEE:
     i. dan kan dit Werkstation direct naar de reparateur.
6. Tijdens het onderzoek van stap 5 kan beoordeeld worden dat het defect niet ligt aan de harde schijf. Indien deze schijf demontabel is, dan zal het Werkstation zonder schijf naar de reparateur gestuurd worden en is het onderzoek van stap 5 niet meer nodig.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

7. Indien een werknemer niet meer een Werkstation nodig heeft, bv. omdat de werknemer:
- uit dienst gaat
- een andere functie heeft gekregen binnen het bedrijf
- langdurig ziek is (dan wel zwanger)

dan:

- wordt er een nieuwe gebruiker aangemaakt (in het besturingssysteem)
- wordt het oude account in principe verwijderd, het kan zijn dat er een overgangsperiode nodig is om bij de oude gebruikersgegevens te moeten komen. Er wordt in dit geval wel vastgelegd hoe lang deze overgangsperiode noodzakelijk is.

Medewerkers mogen met toestemming van de DIR telewerken. Medewerker nemen dan hun draagbare Werkstation, in principe, mee naar huis. Des te minder Workstations er op het bedrijf zijn, des te minder risico en effort er nodig is om eventuele schade door een inbreuk te herstellen.

3.2.2 Doorgevoerde beveiligingsmaatregelen m.b.t. Smartphones

- iedere Smartphone is beveiligd met een uniek wachtwoord,
- Indien gezichts- of vingerafdruk-herkenning mogelijk is wordt deze beveiliging gehanteerd (i.p.v. het wachtwoord),
- iedere Smartphone zal na maximaal 5 minuten in de slaapstand gezet worden, de ICT-specialist zal dit instellen, de gebruiker van de smartphone mag dit niet wijzigen,
- er wordt gebruik gemaakt van Microsoft Exchange Server voor de email. De ICT-specialist heeft daarmee de mogelijkheid om mail op afstand te verwijderen van de smartphone.

Deze maatregelen worden structureel doorgevoerd. Gebruikers van Smartphones moeten bewust van de noodzaak daarvan worden gemaakt.

3.2.3 Doorgevoerde beveiligingsmaatregelen m.b.t. e-mailen

Voor e-mailen van persoonsgegevens geldt dat deze in een excell bestand zijn opgenomen en opgeslagen en dat de gegevens altijd als een bijlage wordt verstuurd.

Voor het e-mailen wordt gebruik gemaakt van Outlook Express dat op alle

werkstations van de werknemers van Stichting Steenbreek is geïnstalleerd.

3.2.4 Doorgevoerde maatregelen m.b.t. telewerken.

Indien gewerkt wordt via internet(-verbindingen), gelden de volgende maatregelen:

1. medewerkers mogen thuiswerken,
2. medewerkers hebben de mogelijkheid om (ook) van andere locaties te werken,
3. medewerkers mogen geen gebruik maken van publieke netwerken zonder beveiliging, hieronder vallen ook gast-wifi-netwerken. Mocht er geen andere optie zijn, dan dient men de roaming (hotspot) functionaliteit van zijn of haar eigen mobiel te gebruiken. Deze mag niet gedeeld worden met anderen,
4. medewerkers die thuiswerken mogen geen privé gegevensdragers en/of andere opslagmedia gebruiken voor werk. Alleen het Werkstation en de smartphone (in bruikleen) mogen gebruikt worden voor opslag van code, data en/of documenten,

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl

5. persoonlijke apparatuur mag niet gebruikt worden voor werkgerelateerde zaken. Denk hierbij aan een personal computer voor thuis. Ook geldt dit voor niet-fysieke middelen zoals; persoonlijke e-mailadressen en/of telefoonnummers.
6. medewerkers die thuiswerken worden geacht om hun eigen netwerk goed te hebben beveiligd, met min. WPA encryptie voor het WIFI-netwerk

Werken via een VPN verdient de voorkeur omdat de beveiliging centraal geregeld kan worden.

3.2.5 Doorgevoerde maatregelen m.b.t. printers.

Vanuit verschillende werkplekken kan geprint worden naar 1 centrale printer. Indien een medewerker persoonsgegevens gaat printen dan is de afspraak dat deze medewerker direct zijn printwerk ophalen dit ter voorkoming van inzage door onbevoegden en derden.

3.2.6 Doorgevoerde maatregelen m.b.t. applicaties

Hier worden applicaties bedoeld die persoonsgegevens bevatten of verwerken:

1. een gebruiker moet ten minste eens per jaar haar of zijn wachtwoord wijzigen. Dit wordt geautomatiseerd afgedwongen in de applicatie. Indien dit laatste niet mogelijk is, dan wordt dit procedureel afgesproken met alle medewerkers,
2. indien de applicatie Two-factor-authenticatie ondersteunt, dan dient dit middel altijd ingezet te worden,
3. indien de applicatie geen Two-factor authenticatie ondersteunt en het gaat om persoonsgegevens betreffende de bijzondere categorieën, dan dient de leverancier deze optie te ontwikkelen.

3.2.7 Doorgevoerde fysieke maatregelen (op kantoor eigen Bedrijf)

Check-Privacy adviseert als standaard om alle applicaties onder te brengen bij een Cloud leverancier. Hierbij gaan wij dan uit van eigen *dedicated servers*! De voordelen hiervan zijn:

1. superieure bewaking in de vorm van:
a. groot hek om het datacenter,
b. gesloten ruimtes alleen toegankelijk met speciale pasjes,
c. cameratoezicht,
d. 24 uur bewaking.
2. (vaak) goedkoper!

Het nadeel is:

1. lagere performance (trager),
2. Het (moeten) afsluiten van een Verwerkersovereenkomst.

Indien de server(s) op een eigen locatie zijn geplaatst dan:

1. dient de server in afgesloten ruimte te staan,
2. dient deze ruimte goed geventileerd te worden,

3. dient de server niet op de grond te staan, vanwege gevaar m.b.t. waterschade,
4. dient de backup buitenshuis bewaard te worden.

3.2.8 Doorgevoerde maatregelen maatregelen m.b.t. het netwerk

De volgende maatregelen worden/zijn doorgevoerd:

1. er zijn twee aparte WIFI netwerken beschikbaar:
a. voor alle medewerkers is er een wifi-verbinding met user en password ingericht,
b. voor gasten is er een openbare wifi-verbinding beschikbaar,
2. voor deze twee WIFI netwerken dienen 2 routers beschikbaar te zijn. Vanuit security is het niet aan te bevelen om met 1 router te werken die 2 verbindingen kan leveren.

3.3. Back-up's, vernietiging van data en audit bestanden

De meest basale veiligheidsmaatregel voor databestanden, is "borgen":

1. iedere nacht wordt er één of meerdere- back-up' s gemaakt,
2. op deze back-up 's worden opgeslagen:
a. de database,
b. de files-directory met oa. Word, Excel, PDF documenten,
c. alle mailwisseling,
3. logbestanden m.b.t. gebruikers betreft informatie welke exacte gebruiker persoonsgegevens heeft geraadpleegd, gewijzigd en/of verwijderd):
a. indien de applicatie deze gegevens kan back-uppen, dan dient dit ook uitgevoerd te worden,
b. Indien de applicatie persoonsgegevens verwerkt van de bijzondere categorieën, dan moet de applicatie deze logbestanden ook back-uppen.
4. Logbestanden m.b.t. systeembeheerders / applicatieontwikkelaars: informatie welke acties zijn ondernomen die in verband staan met persoonsgegevens:
a. indien de applicatie deze gegevens kan back-uppen, dan dient dit uitgevoerd te worden,
b. Indien de applicatie persoonsgegevens verwerkt van de bijzondere categorieën, dan moet de applicatie deze logbestanden back-uppen,
c. de systeembeheerder c.q. applicatie ontwikkelaar moet deze gegevens niet kunnen muteren.

5. De bewaartermijn van de back-up's zijn vastgesteld en staan vermeld in de registers.

STICHTING STEENBREEK • Paulus Borstraat 41 • 3812 TA Amersfoort • T 033 4794050 • E info@steenbreek.nl • W www.steenbreek.nl