AVG

en jouw organisatie

WAT IS AVG EN WAT BETEKENT DAT VOOR MIJN ORGANISATIE?

Met de komst van de Algemene Verordening Gegevensbescherming (AVG) verandert er veel met betrekking tot verwerking en bescherming van persoonsgegevens. Bedrijven die vanaf 25 mei 2018, de datum waarop de AVG van kracht is, niet voldoen aan deze nieuwe privacywetgeving kunnen hoge boetes krijgen, oplopend tot 20 miljoen euro of 4% van de wereldwijde omzet.

De *AVG* (in het Engels *General Data Protection Regulation* of GDPR) vervangt de verouderde Nederlandse Wet bescherming persoonsgegevens (Wbp) en heeft als doel persoonsgegevens beter te beschermen en de bescherming in de Europese Unie (EU) te harmoniseren. De Autoriteit Persoonsgegevens (AP) houdt toezicht op naleving van de AGV.
De nieuwe en strengere Europese wet geldt voor alle organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen. Onder persoonsgegevens vallen 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. Naast naam- en adresgegevens betreft het dus ook medische data, klantprofielen en klikgedrag.
Hoewel sommige bedrijven denken dat ze niks met persoonsgegevens doen, is het goed om inzicht te krijgen of aan alle regels en onderdelen in de AVG wordt voldaan. Worden er persoonsgegevens verwerkt? En zo ja, wat voor gegevens zijn het? Met welk doel worden ze verwerkt? Wat houdt die verwerking in? En waar worden de gegevens bewaard? Het is belangrijk dat bedrijven bij de toezichthouder kunnen aantonen ze *'in control'* zijn. Organisaties moeten duidelijk maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data worden bewaard. Ook moeten ze personen desgevraagd inzage geven in de opgeslagen data.
Daarom is het belangrijk om alle mogelijke bedreigingen ten aanzien van privacy en databeveiliging in kaart te brengen en daarop nieuw of aangepast beleid op te stellen. Dat betekent ook dat met de komst van de AVG praktisch elke organisatie zijn privacyverklaring moet herzien. Deze moet onder de AVG niet alleen meer gedetailleerde informatie bevatten, maar ook in begrijpelijke taal zijn geschreven. De tekst moet toegankelijk en eenvoudig geschreven zijn en begrijpelijk zijn voor de doelgroep waarop een bedrijf zich richt.

Inhoudsopgave

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) – GELDEND PER 25 MEI 2018
Dit document biedt een beknopte handleiding ten aanzien van de AVG. Hieraan kunnen geen rechten worden ontleend. Voor eventuele vragen kunt u contact opnemen met NVPI of een gespecialiseerd adviseur. De eerste twee pagina's van dit document bieden een kort overzicht van de belangrijkste onderwerpen, met verwijzingen naar de volgende pagina's voor verdergaande uitleg en informatie.

Wat zijn persoonsgegevens? Gegevens die betrekking hebben op geïdentificeerde of identificeerbare personen, zoals klanten of medewerkers. Het gaat niet om gegevens over organisaties of bedrijven.

Wat is "verwerken van persoonsgegevens": het verzamelen, vastleggen, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, wissen en vernietigen van persoonsgegevens.

Belangrijke uitgangspunten:

- Bij verwerking met laag risico zijn minder strenge maatregelen nodig dan bij risicovolle verwerking. Bijvoorbeeld de ledenlijst van voetbalvereniging (laag risico) vs financiële gegevens of gegevens over kinderen (hoger risico).
- Bij het ontwikkelen van nieuwe producten, systemen en processen: zoveel mogelijk pseudonimiseren, anonimiseren en overbodige gegevens verwijderen. Als standaardinstelling de meest privacy-vriendelijke optie instellen.

Zie A >

CONCRETE ACTIES / VERPLICHTINGEN

1. VERWERKINGENREGISTER: alle verwerkingen registreren en met het register kunnen aantonen dat de verwerkingen conform de regels zijn.

Zie B >

2. GRONDSLAG VOOR DE VERWERKING: om te mogen verwerken moet er tenminste één van de in de wet aangegeven grondslagen zijn. Mogelijke grondslagen zijn:

Zie C >

a. toestemming van de betrokkene voor de verwerking,

Zie D >

b. een wettelijke verplichting (zoals scan identiteitsbewijs van personeel in loonadministratie),
c. nodig voor het uitvoeren van een overeenkomst met betrokkene, bijvoorbeeld een klant,
d. gerechtvaardigd belang van de verwerkingsverantwoordelijke.

Zie E >

3. PRIVACY STATEMENT OP WEBSITE.

Zie F >

4. RECHT VAN BETROKKENEN

a. inzage,
b. rectificatie,
c. verwijdering (in bepaalde gevallen),
d. dataportabiliteit (opvragen/doorgeven gegevens),
e. niet-onderwerping aan bepaalde profilering,
f. het maken van bezwaar.

Zie G >

5. EEN PRIVACY IMPACT ASSESSMENT (PIA) oftewel een (zelf op te stellen) "gegevens-beschermingseffectbeoordeling", is verplicht indien de verwerking een hoog risico heeft met name bij nieuwe technologieën en gelet op de aard, omvang en context van de doelen. Is er geen hoog risico dan is een PIA niet verplicht.

Een PIA moet resulteren in (a) een beschrijving van de boogde

verwerking en de doelen daarvan, (b) een oordeel over de noodzakelijkheid en evenredigheid van de verwerking met het oog op het vastgestelde doel, (c) een oordeel over de risico's voor betrokkenen, en (d) de beoogde maatregelen waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen. Deze uitkomst moet worden meegenomen bij het vaststellen van de maatregelen ter bescherming van de betrokkene en om aan te tonen dat de AVG wordt nageleefd.

Zie H >

6. PASSENDE TECHNISCHE EN ORGANISATORISCHE BEVEILIGING IS VERPLICHT. Wat passend is hangt af van een zelf uit te voeren risicovaststelling. Bij risico's gaat het bijvoorbeeld om materiele of immateriële schade, die zich kan voordoen doen bij verlies, wijziging of toegang tot de persoonsgegevens. Van een verhoogd risico is bijvoorbeeld sprake als het gaat om gegevens van kinderen, een grote hoeveelheid gegevens of betrokkenen, of profiling.

Passende maatregelen kunnen zijn: pseudonimisering, versleuteling, het vermogen om permanent de vertrouwelijkheid van de verwerkingssystemen en diensten te garanderen.

Technische maatregelen kunnen bijvoorbeeld zijn een firewall en beveiligde omgevingen. Organisatorische maatregelen kunnen bijvoorbeeld zijn: het beperken van de toegang tot gegevens tot bepaalde medewerkers (autorisatiebeleid), toegangscontrole met wachtwoorden, logging van handelingen rondom persoonsgegevens en toegangsbeveiliging pand, beveiliging van netwerkverbindingen en beheer van kopieën en back-ups.

Zie I >

7. PROTOCOL DATALEKKEN: binnen 72 uur moet een lek gemeld worden bij de Autoriteit Persoonsgegevens. Er is geen meldplicht indien het onwaarschijnlijk is dat er een risico is voor individuen, bijvoorbeeld bij een verloren USB-stick met namen van meerderjarige leden van een voetbalvereniging. Ook het type en aantal gegevens is daarbij van belang.

Ook moet een datalek "onverwijld" worden gemeld bij de betrokkene als het lek een *hoog risico* met zich meebrengt zodat betrokkene de nadelige gevolgen zo veel mogelijk kan beperken of voorkomen. Zoals bij een gestolen database met inloggegevens, een gehackte website, vernietigde host-omgeving zonder back-up, onbevoegde toegang tot financiële informatie. Er is geen meldplicht aan de betrokkene als er (a) passende technische en organisatorische beschermingsmaatregelen zijn genomen bijvoorbeeld door versleuteling van de gegevens, (b) achteraf maatregelen zijn genomen waarmee de risico's voor betrokkenen zijn weggenomen, (c) mededeling aan betrokkene onevenredig veel inspanning zou kosten in welk geval een openbare mededeling volstaat (bijvoorbeeld publicatie op website).

Er moet een register worden bijhouden van datalekken. Met informatie over detectie, analyse, beoordeling en verbeteringen.

8. HET AANSTELLEN VAN EEN FUNCTIONARIS GEGEVENSBESCHERMING is verplicht indien de verwerkingsverantwoordelijke "hoofdzakelijk is belast met verwerkingen die vanwege aard, omvang en/of doelen regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen". Voorbeelden zijn het online volgen of profiling, het tonen van advertenties op basis van internetgebruik, klantenkaarten of lokalisering met mobiele apps.

Zie J >

9. ER MOET EEN VERWERKERSOVEREENKOMST ZIJN indien een derde partij persoonsgegevens verwerkt in opdracht en volgens instructies. Zoals een telemarketingbedrijf of een searchoptimalisatiebureau.
De verwerkersovereenkomst moet aan specifieke eisen voldoen.

Zie K >

A - INLEIDING

- **Persoonsgegevens** Een *combinatie van gegevens* zijn ook persoonsgegevens indien de combinatie leidt tot identificeerbaarheid. Een IP-adres is ook een persoonsgegeven.

- **Risico-gebaseerde benadering.** Bij het nemen van vereiste maatregelen ter bescherming van persoonsgegevens moet rekening worden gehouden met de aard, omvang, context en doel van de verwerking en de waarschijnlijkheid en ernst van de risico's voor de betrokken personen bij misbruik van de gegevens. Bij een laag risico (bijvoorbeeld de ledenlijst van voetbalvereniging) zijn minder verstrekkende maatregelen nodig dan bij risicovolle verwerking (bijvoorbeeld een ziekenhuis met medische gegevens). Voorbeelden van gegevens met hoog risico zijn financiële gegevens en gegevens over kinderen.

- **Verwerken van bijzondere persoonsgegevens** is in principe verboden. Dat zijn gegevens over ras, etnische afkomst, politieke of religieuze overtuigingen, lidmaatschap vakbond, genetische of biometrische gegevens, seksuele geaardheid en gezondheid. Strafrechtelijke gegevens of ten aanzien van bepaalde rechterlijke verboden mogen alleen worden verwerkt onder toezicht van de overheid of indien in de wet geregeld. Het BSN nummer mag niet worden gebruikt tenzij door de overheid of voor specifiek voor het BSN nummer in de wet of AMvB voorgeschreven doelen.

- **Beginselen van de wet**
  De AVG kent belangrijke "beginselen" die in de AVG zijn uitgewerkt, ter bescherming van persoonsgegevens:
  a. Rechtmatigheid, behoorlijkheid en transparantie.
     Doelbinding. Alleen gegevens verwerken voor een bepaald doel.
  c. Minimale gegevensverwerking. Aantal en omvang beperken tot wat nodig is.
  d. Juistheid. Recht op rectificatie.
  e. Opslagbeperking. Niet langer bewaren dan voor het doel nodig is.
  f. Bij het ontwikkelen van beleid en product-of systeemontwerp moeten organisatorische en technische maatregelen worden genomen. Dit wordt *privacy by design* genoemd (bijvoorbeeld: zoveel mogelijk pseudonimiseren, anonimiseren en overbodige gegevens verwijderen) en *privacy by default:* kiezen voor de meest privacy-vriendelijke optie als standaardinstellingen.

B - VERWERKINGENREGISTER

De verwerkingsverantwoordelijke moet kunnen aantonen dat alle verwerkingsactiviteiten volgens de AVG plaatsvinden. Daarbij geldt de risico-gebaseerde benadering: bij meer risico zijn verdergaande maatregelen vereist dan bij een lager risico.

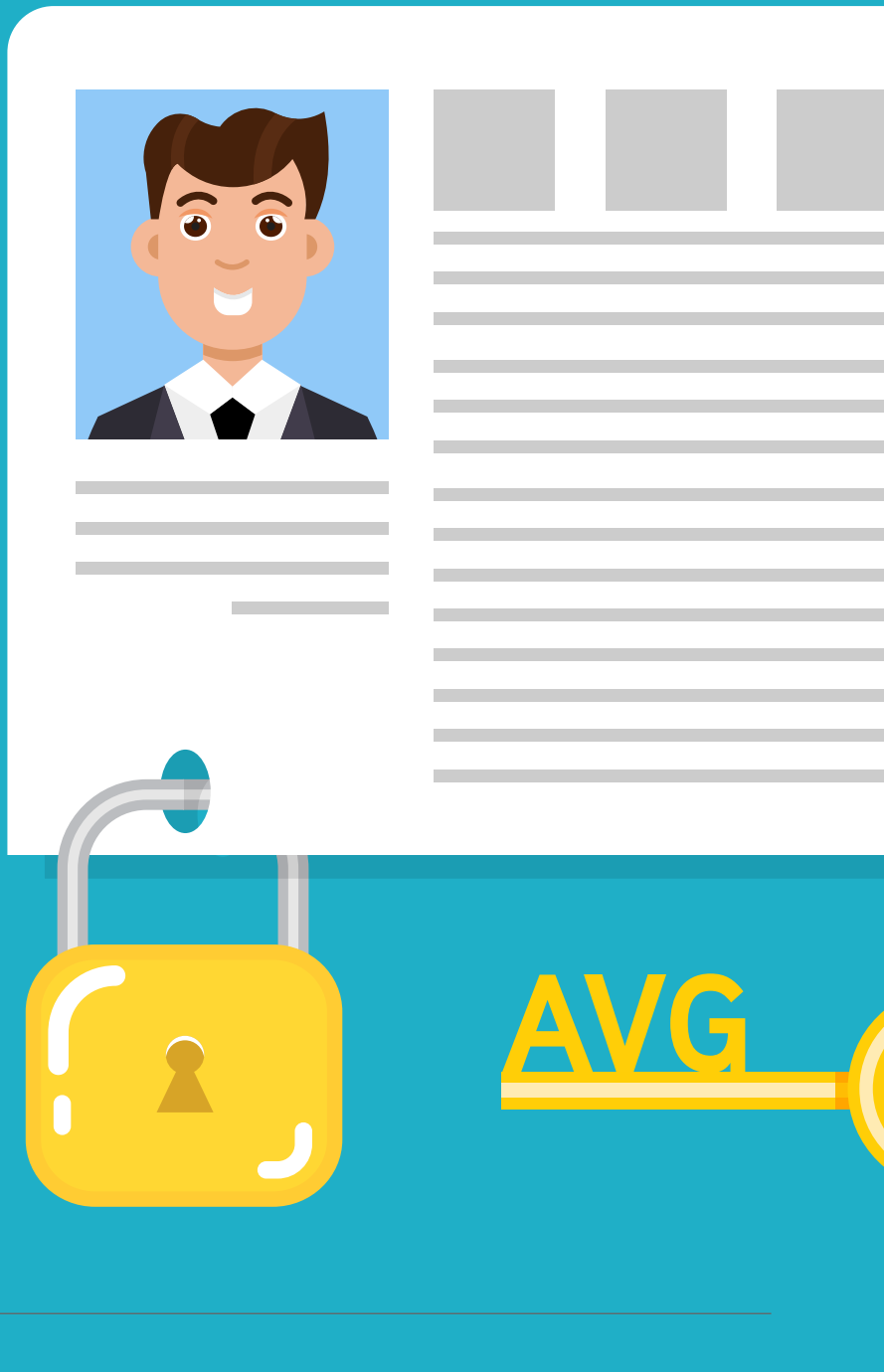
De verwerkingsverantwoordelijke moet een (intern) verwerkingenregister bijhouden met de volgende informatie:

a. Naam en contactgegevens van de verwerkingsverantwoordelijke.
b. Contactgegevens Functionaris Gegevensbescherming (indien van toepassing).
c. Verwerkingsdoel(en).
d. Categorieën persoonsgegevens.
e. Categorieën betrokkenen.
f. Categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt.
g. Bron van de gegevens.
h. Beoogde bewaartermijn.
i. Of de persoonsgegevens worden gedeeld buiten de EU. Zo ja, dan documenten inzake passende waarborgen vermelden.
j. Indien mogelijk: algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.

Bij wijzigingen moet het register worden bijgewerkt. De Autoriteit Persoonsgegevens en de Functionaris Gegevensbescherming (zie onder) moeten desgevraagd toegang hebben tot het register.

Nieuw maar verenigbaar doel: Indien de gegevens voor een ander doel worden gebruikt dan tijdens het verkrijgen van de persoonsgegevens is gemeld, moet de verwerkings-verantwoordelijke beoordelen of het nieuwe doel verenigbaar is met het eerdere doel. Daarbij moet rekening worden gehouden met:

a. Verband tussen de doelen.
b. Het kader waarin de persoonsgegevens zijn verzameld,
met name wat de verhouding tussen de betrokkenen en
de verweringverantwoordelijke betreft.
c. De aard van de persoonsgegevens, met name of bijzondere categorieën persoonsgegevens worden verwerkt.
d. De mogelijk gevolgen van de voorgenomen verdere verwerking voor de betrokkenen.
e. Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.



C - GRONDSLAG

Er dient tenminste één grondslag te zijn voor de verwerking van persoonsgegevens.
Mogelijke grondslagen zijn:

a. Toestemming van betrokkene, of
b. Wettelijke verplichting. Bijvoorbeeld scan van een identiteitsbewijs van personeel in loonadministratie, of
c. Noodzakelijkheid voor uitvoeren van een overeenkomst. Bijvoorbeeld een arbeidsovereenkomst voor wat betreft het verwerken van salaris- en bankgegevens, of
d. Noodzakelijkheid voor een gerechtvaardigd belang van de verwerkings-verantwoordelijke, mits de belangen, rechten en vrijheden van betrokkene niet zwaarder wegen met name wanneer betrokkene een kind is.
    - Deze afweging moet de verwerkingsverantwoordelijke zelf maken. Hoe gevoeliger de persoonsgegevens zijn, hoe zwaarder het belang van de betrokkene weegt. Aan de andere kant: hoe sterker de maatregelen zijn, hoe eerder de verwerking kan worden gebaseerd op deze grondslag.
    - De betrokkene moet bezwaar kunnen maken, waarna een nieuwe afweging nodig is.
    - Direct-marketing is een gerechtvaardigd belang, maar zodra de betrokkene hiertegen bezwaar maakt moet de verwerking stoppen.
e. Noodzakelijk om de vitale belangen van betrokkene of ander natuurlijk persoon te beschermen.
f. Noodzakelijk voor een taak van algemeen belang of taak in het kader van uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijk is opgedragen.

D - TOESTEMMING

Eén van de grondslagen voor het mogen verwerken is toestemming van de betrokkene. Er gelden specifieke eisen voor toestemming:

a. Toestemming door actieve handeling (bijv. door de betrokkene zelf aanvinken).
b. Geïnformeerde toestemming. De betrokkene moet geïnformeerd worden over:
   I. doel,
   II. wijze van verwerken,
   III. met wie delen,
   IV. bewaartermijn,
   V. Of gegevens naar buiten de EU gaan?

Zie ook Model Privacy Statement.

c. Verwerkingsverantwoordelijke moet kunnen bewijzen dat en waarvoor toestemming is verkregen. Bijvoorbeeld door informatie vast te leggen over het websitebezoek waarin de toestemming is verleend. Deze informatie is te combineren met documentatie over het proces op welke manier toestemming is ontvangen. Bijvoegen van een kopie van de informatie die de betrokkenen hebben ontvangen voorafgaand aan de gegeven toestemming. Het verwijzen naar automatische registratie van toestemming door een website is onvoldoende om geldige toestemming aan te kunnen tonen (aan het vereiste van "geïnformeerde toestemming" is dan niet voldaan).
d. Toestemming moet duidelijk en eenvoudig zijn.
e. Toestemming moet net zo makkelijk zijn in te trekken als te verstrekken.
f. Toestemming moet 'vrij' gegeven zijn.
   – Toestemming moet een vrije keus zijn (geen druk, dwang of anderszins niet vrij). Toestemming van een werknemer aan een werkgever wordt geacht niet 'vrij' te worden gegeven vanwege gezagsverhouding (bepaalde uitzonderingen zijn mogelijk).
   – Bij de beoordeling of toestemming 'vrij' verleend is, moet "ten sterkste" rekening worden gehouden met de vraag of de verwerking waarvoor toestemming wordt gevraagd vereist is voor uitvoering van de overeenkomst.
   – Mag geen (niet onderhandelbaar) onderdeel zijn van algemene en/of gebruiksvoorwaarden.
   – Een weigering van toestemming mag geen nadelige gevolgen hebben voor betrokkene.
g. Toestemming van ouders bij kinderen <16 jaar in geval van "een rechtsreeks aanbod van diensten van de informatiemaatschappij" aan een kind. Bijvoorbeeld bij online verkopen. Vaststelling of de ouders toestemming hebben gegeven vereist een redelijke inspanning, met inachtneming van de beschikbare technologie, om te controleren dat de toestemming inderdaad door degene die de ouderlijke verantwoordelijkheid draagt is gegeven.

E - GERECHTVAARDIGD BELANG

Noodzakelijkheid voor een gerechtvaardigd belang van de verwerkingsverantwoordelijke, mits de belangen, rechten en vrijheden van betrokkene niet zwaarder wegen met name wanneer betrokkene een kind is.

- Deze afweging moet de verwerkingsverantwoordelijke zelf maken.
  Hoe gevoeliger de persoonsgegevens zijn, hoe zwaarder het belang van de betrokkene weegt.
  Aan de andere kant: hoe sterker de maatregelen zijn, hoe eerder de verwerking kan worden gebaseerd op deze grondslag.
- De betrokkene moet bezwaar kunnen maken, waarna een nieuwe afweging nodig is.
- Direct-marketing is een gerechtvaardigd belang van de verwerkingsverantwoordelijke, maar zodra de betrokkene hiertegen bezwaar maakt moet de verwerking stoppen.

F - RECHT OP INFORMATIE
(ZIE: MODEL "PRIVACY STATEMENT")

Betrokkenen hebben het recht te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's, de regels die gelden, de waarborgen en de manier waarop zij hun rechten kunnen uitoefenen.

De informatie moet worden verstrekt bij het verkrijgen van de persoonsgegevens. In de bijlage vindt u deze informatie in de vorm van een model Privacy Statement. De informatie moet, in het bijzonder indien de informatie voor een kind bestemd is, gevat zijn in "beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal".

Als de persoonsgegevens voor andere doelen gaan worden verwerkt, dan moet de betrokken opnieuw worden geïnformeerd over dat nieuwe doel en opnieuw alle informatie worden verstrekt, behalve voor zover de betrokkene al van die informatie op de hoogte is.

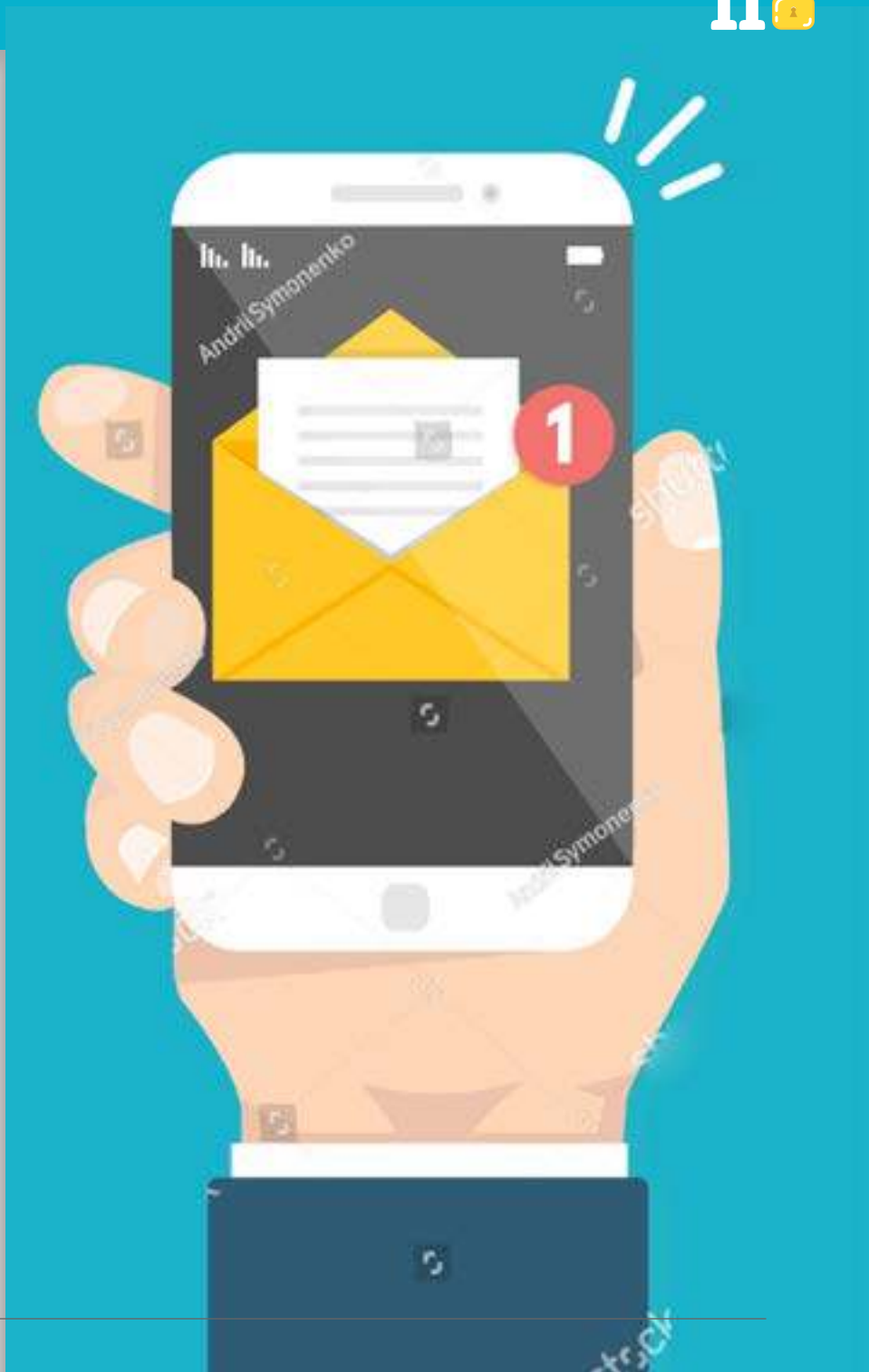
Indien de persoonsgegevens niet van betrokkene afkomstig zijn moet de betrokkene binnen een maand geïnformeerd worden en indien de gegevens worden gebruik voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met betrokkene. Indien de gegevens aan een andere ontvanger worden verstrekt geldt uiterlijk het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt. Indien betrokkene al over de benodigde informatie beschikt, hoeft niet geïnformeerd te worden. Daarvan mag worden uitgegaan als naar objectieve maatstaven uit een gedraging of verklaring van betrokkene kan worden afgeleid dat deze inderdaad op de hoogte was. Dit is bijvoorbeeld het geval als de informatie eerder aan betrokkene is verstrekt door middel van een e-mail gericht aan een door betrokkene zelf opgegeven e-mailadres. Ook hoeft in bepaalde gevallen niet geïnformeerd te worden indien dat "onmogelijk blijkt of onevenredig veel inspanning zou vergen", of voor zover de verwezenlijking van de doelen van de verwerking daardoor onmogelijk dreigt te worden gemaakt of ernstig in het gedrang dreigen te worden gebracht (in dergelijke gevallen "neemt de verwerkingsverantwoordelijke passende maatregelen, om de rechten, de vrijheden en de gerechtvaardigde belangen van betrokkene te beschermen, waaronder et openbaar maken van de informatie").

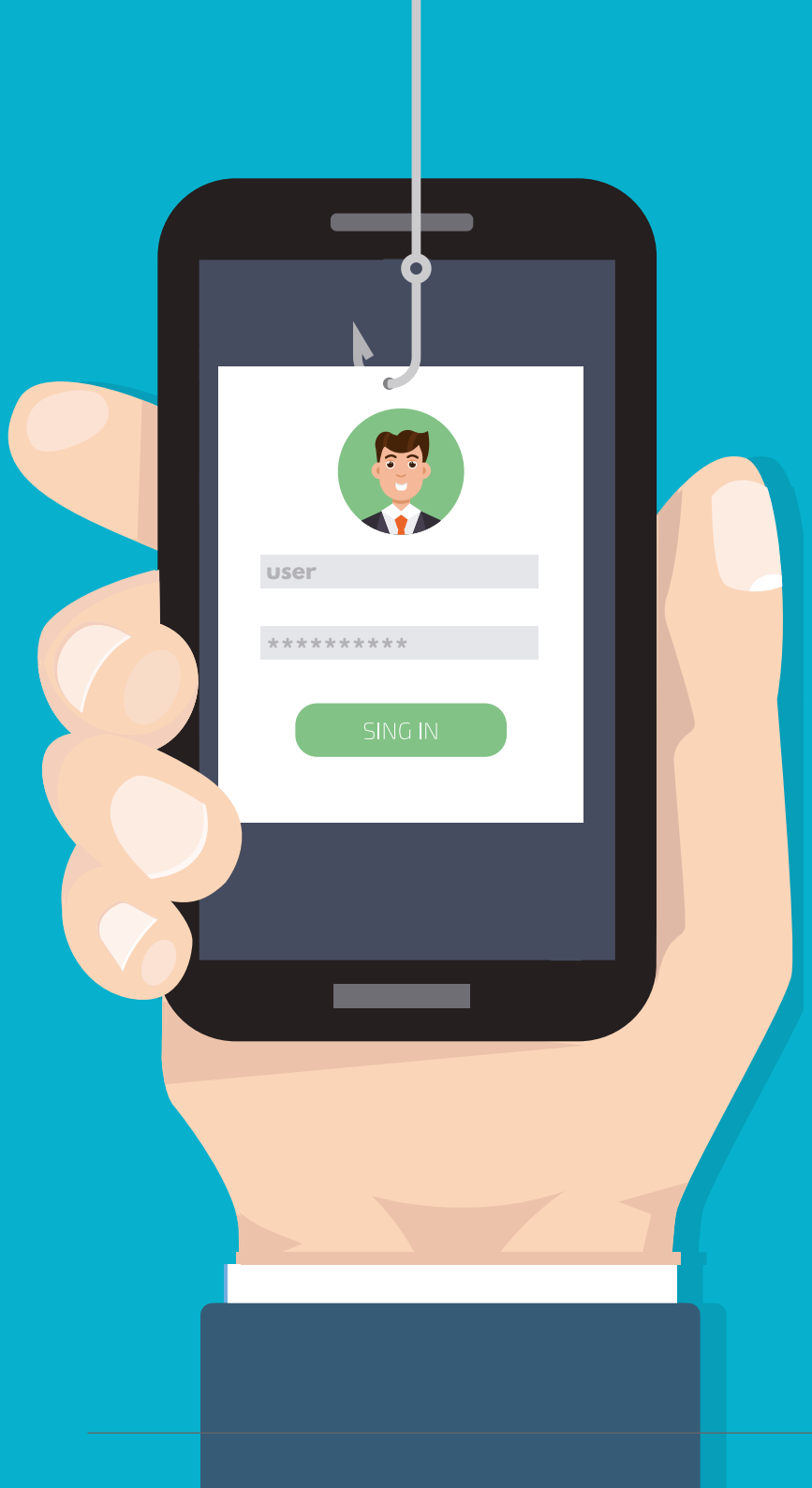
G - RECHTEN VAN BETROKKENE(N)

Betrokkenen hebben op grond van de AVG de volgende rechten die zij kunnen uitoefenen.

a. Recht op informatie (zie punt F hiervoor).
b. Recht op inzage.
c. Recht op rectificatie. Als gegevens niet kloppen. Rectificaties moeten door verwerkingsverantwoordelijke verstrekt worden aan ieder die de persoonsgegevens ontvangen heeft. Ook moet de betrokkene daarover desgevraagd worden geïnformeerd.
d. Recht op verwijdering van de gegevens in de volgende gevallen:
   I. Als gegevens niet langer nodig zijn voor het doel.
   II. Bij intrekking toestemming indien dat enige verwerkingsgrondslag is.
   III. Na gegrond bezwaar tegen de verwerking.
   IV. Onrechtmatige verwerking.
   V. Om te voldoen aan wettelijke verplichting.
   VI. Indien de persoonsgegevens zijn verzameld in verband met aanbod van internetdiensten aan een kind (zoals online verkopen).

Recht om vergeten te worden: zodat mensen op het internet niet voor altijd (ten onrechte) met hun verleden worden geconfronteerd. De verwerkings-verantwoordelijke moet “redelijke technische en organisatorische maatregelen nemen om andere verwerkingsverantwoordelijken ervan op de hoogte te stellen dat betrokkene vergeten wil worden.





Dit betekent dat iedere koppeling naar en kopie of reproductie van de gegevens gewist moet worden. Het recht op verwijdering en recht om vergeten gelden niet indien de verwerking nodig is voor het “uitoefenen van het recht op vrijheid van meningsuiting en informatie”.

e. Recht op beperking van verwerking. Het tijdelijk on hold zetten van de verwerking. Dit recht geldt in bepaalde gevallen (zoals tijdens het beroep op rectificatie).
f. Recht van bezwaar. Er moet worden gestopt met verwerking tenzij er dwingende gerechtvaardigde gronden zijn voor de verwerking die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. Ingeval van direct marketing moet na bezwaar de verwerking voor dat doel *altijd* worden beëindigd.
g. Recht op dataportabiliteit. De persoonsgegevens moeten door betrokkene of door de betreffende andere verwerkingsverantwoordelijke kunnen worden verkregen “in een gestructureerde, gangbare en machine-leesbare vorm”. Om te bevorderen dat betrokkene kan overstappen naar een andere verwerkingsverantwoordelijke dienstverlener. Dit recht geldt allen bij rechtsgronden “toestemming” of “noodzakelijkheid voor uitvoering van een overeenkomst”. Het betreft alleen gegevens die betrokkene zelf heeft aangeleverd (zoals inloggegevens) en gegevens die gegenereerd zijn door gebruik (bijvoorbeeld luister- of kijkgedrag bij een streamingdienst, zoekgeschiedenis of klikgedrag). Hieronder valt niet profielinformatie of analyse n.a.v. gedrag van het individu.
h. Recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking (waaronder profilering) gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Uitzonderingen zijn (o.a.) verkregen toestemming of indien noodzakelijk voor een overeenkomst tussen betrokkene en verwerkingsverantwoordelijke).

H - PRIVACY IMPACT ASSESSMENT (PIA)

a. Een PIA is verplicht indien een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen, in het bijzonder wanneer nieuwe technologieën worden gebruikt, en gelet op de aard, omvang en context en doelen.

b. Er is in ieder geval sprake van een hoog risico in deze gevallen:
   1. Geautomatiseerd systematisch persoonlijke aspecten evalueren waaronder profilering en op basis daarvan besluiten nemen met rechtsgevolgen voor betrokkene.
   2. Op grote schaal verwerken van bijzondere of strafrechtelijke persoonsgegevens.
   3. Grootschalig en stelselmatig mensen volgen in openbaar (zoals cameratoezicht).
   4. Ook hoog risico in geval verwerking voldoet aan twee of meer van onderstaande criteria:
      I. Evaluatie van personen of scoretoekenning.
      II. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar gevolg.
      III. Stelselmatige monitoring.
      IV. Gevoelige gegevens of gegevens van zeer persoonlijke aard.
      V. Op grote schaal verwerkte gegevens. Matching of samenvoeging van datasets.
      VI. Gegevens met betrekking tot kwetsbare betrokkenen.

VI. Innovatieve toepassing van nieuwe technologische of organisatorische oplossing.
VIII. Blokkering van een recht, dienst of contract.

De toezichthoudende Autoriteit Persoonsgegevens publiceert lijsten met daarop verwerkingen waarvoor een PIA verplicht is.

De PIA moet resulteren in:
- Een beschrijving van de beoogde verwerking en de doelen daarvan.
- Een oordeel over de noodzakelijkheid en evenredigheid van de verwerking met het oog op het vastgestelde doel.
- Een oordeel over de risico's voor betrokkenen. Daarbij moeten de volgende omstandigheden worden meegenomen: (a) aard van de gegevensverwerking, (b) omvang, context en doelen van de verwerking en (c) de bronnen van de risico's.

In een PIA moeten met name de oorsprong, aard, specifieke karakter en de ernst van risico's voor de betrokkenen worden geanalyseerd. Daarbij moeten de specifieke waarschijnlijkheid en de ernst van de risico's voor de persoonlijke levenssfeer van de betrokkenen worden beoordeeld.

Onderzocht moet worden of de geplande maatregelen, waarborgen en mechanismen om de belangen van betrokkene te beschermen voldoende zijn, dan wel of verbetering mogelijk is waarmee de risico's voor betrokkene worden beperkt. De resultaten van de PIA moeten regelmatig worden geëvalueerd met het oog op veranderde omstandigheden.

De resultaten van de PIA moeten worden meegenomen bij het vaststellen van de maatregelen om de belangen van betrokkenen te beschermen en om aan te tonen dat de AVG wordt nageleefd.

I - BEVEILIGING

Het is verplicht om passende technische en organisatorische maatregelen te nemen. Wat passend is hangt af van een risicovaststelling.

a. Bij risico's moet gedacht worden aan lichamelijk, materiele of immateriële schade, die zich voor kunnen doen bij verlies, vernietiging, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot de persoonsgegevens.
b. Van dergelijke risico's is voornamelijk sprake wanneer de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid bij beroepsgeheim, ongeoorloofde ongedaanmaking van pseudonimisering en enig ander aanzienlijk economisch of maatschappelijk nadeel.

c. Een verhoogd risico wordt in ieder geval aangenomen wanneer
   I. de betrokkenen rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen,
   II. het gegevens betreft over ras, etnische afkomst, politieke opvattingen, religie, vakbondslidmaatschap, genetische gegevens of over gezondheid of seksueel gedrag, of strafrechtelijke gegevens,
   III. persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken,
   IV. wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen worden verwerkt, of
   V. wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heft voor een groot aantal betrokkenen.

Daarnaast dient bij de beoordeling van wat passend is rekening te worden gehouden met:

a. stand van de techniek
b. uitvoeringskosten
c. aard van de verwerking
d. omvang van de verwerking
e. context van de verwerking
f. verwerkingsdoelen
g. ernst van de vastgestelde risico's , en
h. de waarschijnlijkheid dat de risico's zich zullen verwezenlijken.

Passende maatregelen kunnen zijn:

a. Pseudonimisering.
b. Vermogen om permanent de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
c. Vermogen om bij een fysiek of technisch incident de beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen.
d. Procedure voor het testen, beoordelen en evalueren van doeltreffendheid van technische en organisatorische maatregelen ter beveiliging van de verwerking.
e. Encryptie.
f. Firewall of het opslaan van gegevens in beveiligde omgevingen.
g. Beperken van de toegang tot gegevens tot bepaalde medewerkers.
h. Toegangscontrole met wachtwoorden.
i. Logging van handelingen rondom persoonsgegevens.
j. Toegangsbeveiliging pand.
k. Steekproefsgewijze controle op naleving beleid.
l. Beheer van kopieën en backups.
m. Beveiliging van netwerkverbindingen.

Voorafgaande raadpleging Autoriteit Persoonsgegevens

Verwerking van persoonsgegevens moet vooraf worden voorgelegd aan de Autoriteit Persoonsgegevens, indien hoge risico's voor betrokkenen niet worden weggenomen door maatregelen. De Autoriteit persoonsgegevens kan vervolgens advies geven en diverse bevoegdheden uitoefenen die vermeld staan in artikel 58 van de AVG.

J - AANSTELLEN FUNCTIONARIS GEGEVENSBESCHERMING

De Functionaris Gegevensbescherming informeert over de verplichtingen omtrent bescherming van persoonsgegevens, verzamelt informatie over verwerkingsactiviteiten, let op naleving van de regels, adviseert over inzet van persoonsgegevens en overlegt met toezichthouder (Autoriteit Persoonsgegevens). Dit kan een deskundige in loondienst zijn, dan wel via een dienstverleningsovereenkomst. De verwerkingsverantwoordelijke is juridisch verantwoordelijk voor naleving en niet de functionaris.

a. Het aanstellen van een Functionaris Gegevensbescherming is verplicht indien:
   - De verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen die vanwege aard, omvang en/of doelen regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen. Het moet gaan om een kerntaak van de organisatie. Deze omvatten ook alle activiteiten waarbij het verwerken van gegevens onlosmakelijk deel uitmaakt van de activiteit van de verwerkingsverantwoordelijke. Ondersteunende activiteiten zoals uitbetaling van werknemers of standaard IT-ondersteuning vallen daar niet onder.
     - Op grote schaal: grens is nog niet duidelijk. Daarbij weegt (o.a.) mee aantal personen, hoeveel gegevens, duur van de verwerking, lokaal of internationaal). In ieder geval bij zoekmachines, ziekenhuizen, OV, fastfoodketens, verzekeraars, banken, telecom- en internetproviders.
     - Regelmatig en stelselmatig observatie. Bijvoorbeeld volgen en profilering op internet, of het tonen van advertenties o.b.v. internetgebruik. Ook: klantenkaart systemen, lokalisering met mobiele apps.

b. Grootschalige verwerking van bijzondere categorieën persoonsgegevens of strafrechtelijke gegevens.

K - VERWERKERSOVEREENKOMST

De verwerkersovereenkomst moet aan specifieke eisen voldoen, ter waarborging van de bescherming van de persoonsgegevens. Een aantal zaken moeten daarin nader worden geregeld waaronder ten aanzien van de toegang tot de gegevens, geheimhouding, beveiligingsniveau, medewerking bij nakomen van verplichtingen met betrekking tot rechten van betrokkene, verplichtingen in geval van datalekken, en het moeten wissen van gegevens na beëindiging van de samenwerking. De AVG bevat ook enkele verplichtingen die rechtstreeks gelden voor de verwerker (onder andere m.b.t. beveiliging en het verwerkingenregister).

MODEL PRIVACY STATEMENT:

1. Naam en contactgegevens van de verwerkingsverantwoordelijke (bedrijf):

2. *Indien van toepassing:* contactgegevens van de Functionaris Gegevensbescherming:

3. Verwerkingsdoel en rechtsgrond voor de verwerking:

4. *Indien van toepassing:* de gerechtvaardigde belangen van de verwerkingsverantwoordelijke:

5. Categorieën persoonsgegevens:

6. *Indien van toepassing:* ontvangers of categorieën van ontvangers van de persoonsgegevens:

7. *Indien van toepassing:* aangeven voornemen de persoonsgegevens door te geven aan derde land of internationale organisatie.
   - In dat geval ook aangeven of er adequaatheidsbesluit van de Europese Commissie bestaat, of wat de passende waarborgen zijn en hoe daarvan een kopie van kan worden verkregen of waar deze kunnen worden geraadpleegd:

8. Bewaartermijn, indien onmogelijk aan te geven, dan de criteria ter bepaling van die termijn:

9. Betrokkene heeft recht op
   - rectificatie of wissing van de persoonsgegevens
   - beperking van de verwerking
   - recht tegen verwerking bezwaar te maken
   - recht op gegevensoverdraagbaarheid
10. *Indien van toepassing:* betrokkene heeft het recht door hem verleende toestemming in te trekken, zonder dat dit afbreuk doet aan de eerdere rechtmatigheid van de verwerking.
11. Betrokkene heeft recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
12. Vermelden of de verstrekking van persoonsgegevens een wettelijke contractuele verplichting is, of een noodzakelijke voorwaarde om een overeenkomst te sluiten en of betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer de gegevens niet worden verstrekt.
13. *Indien van toepassing:* Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
14. Indien de persoonsgegevens niet van betrokkene zijn verkregen: aangegeven wat de bron is van de gegevens, en of zij afkomstig zijn van openbare bronnen.

NVPI, Hogehilweg 6,
1101 CC Amsterdam
www.nvpi.nl