



Protocol

Algemene Verordening Gegevensbescherming
(AVG)

Versie 102021

Inhoud

Inleiding	4
Digitalisering	4
Verantwoordingsplicht.....	4
Ingangsdatum	4
Verantwoordingsplicht.....	4
Verplichte maatregelen.....	5
Bewustwording	5
1. Verwerkingsregister.....	5
Algemene gegevens	5
Categorie personen en persoonsgegevens.....	5
Algemene gegevens vrijwilligers.....	5
Grondslag van de verwerking.....	6
Doel van verwerking.....	6
Bewaartermijn persoonsgegevens	6
Delen gegevens met derden	6
Maatregelen tegen risico's.....	6
Rol Functionaris Gegevensbescherming.....	7
Bestuursbesluiten rondom de AVG.	7
3. Datalekken.	7
Meldplicht.....	7
Beschrijving datalek	7
Gebruikte termen in wet AVG.....	7
Registratie datalek.....	8
Melden datalek.....	8
Beleidsregels.....	8
Boete	8
Maatregelen tegen datalekken.....	8
Praktische informatie bij malware.....	9
Melden malware datalek	9
4. Toestemmingsverklaring	9
Eisen waar de toestemming aan moet voldoen.	9
Beveiliging & bescherming	10
Portretrecht.....	10
Auteursrecht.	10
5. Functionaris Gegevensbescherming (FG).....	10
AVG en bewaartermijnen.....	10
Bewaartermijn	11
Adresgegevens voor reünies.....	11
Inhoud (digitale) dossiers	11
Nieuwe Europese privacyregels.....	11
Privacy by design.....	11

Privacy by default	11
Privacyverklaring	12
Relevante websites.....	12

Inleiding

Met de komst van de Algemene verordening Gegevensbescherming (AVG) krijgt de stichting Buitenzorg Beheer, de stichting Buitenzorg Dragonder en stichting Buitenzorg Ruisseveen (hierna te noemen de stichting) meer verantwoordelijkheid om de persoonsgegevens van vrijwilligers en sponsoren goed te beschermen.

Digitalisering

De opkomst en het gebruik van innovatieve, digitale systemen biedt de stichting interessante mogelijkheden om de kwaliteit van de activiteiten en de interne werkprocessen te verbeteren en te optimaliseren. Bijvoorbeeld de website van de stichting en het gebruik van sociale media & apps (bijv. Facebook en Whatsapp). Maar deze nieuwe mogelijkheden om persoonsgegevens te verwerken, brengen ook de verantwoordelijkheid met zich mee om dat zorgvuldig en veilig te doen.

Verantwoordingsplicht

Onder de AVG geldt de verantwoordingsplicht. De verantwoordingsplicht houdt onder meer in dat de stichting aan moet kunnen tonen welke technische en organisatorische maatregelen zij heeft genomen om de persoonsgegevens van de vrijwilligers en sponsoren te beschermen.

De stichting moet aan de toezichthouder, de Autoriteit Persoonsgegevens (AP), goed kunnen onderbouwen waarom zij het recht heeft om bepaalde persoonsgegevens te verwerken. In sommige gevallen heeft zij bijvoorbeeld toestemming nodig van vrijwilligers of bezoekers om persoonsgegevens te verwerken. Zoals voor het publiceren van foto's op de website van de stichting waarop vrijwilligers of bezoekers herkenbaar in beeld zijn. De stichting moet dan kunnen aantonen (schriftelijk ondertekend) dat zij die toestemming heeft. In dit AVG-protocol beschrijft de stichting hoe zij hieraan gestalte geeft en toont aan daaraan te voldoen.

Ingangsdatum

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG) en vervalt de Wet Bescherming Persoonsgegevens (WBP).

Verantwoordingsplicht.

De Algemene verordening Gegevensbescherming (AVG) legt meer verantwoordelijkheid bij de stichting om aan te tonen dat zij aan de privacyregels voldoet. De organisatie voldoet aan deze verantwoordingsplicht en beschermt daarmee het grondrecht op privacy van bestuursleden en vrijwilligers.

De stichting heeft in dit document beschreven hoe de persoonsgegevens verwerkt en beschermd worden en toont aan dat de verwerking aan de regels van de AVG voldoet.

Deze beschrijving betreft de volgende gebieden:

- Rechtmatigheid;
- Transparantie;
- Doelbinding;
- Juistheid.

Ook zijn de noodzakelijke technische en organisatorische maatregelen genomen om de persoonsgegevens te beschermen. Zie daarvoor de betreffende hoofdstukken.

Verplichte maatregelen

De Algemene verordening Gegevensbescherming (AVG) benoemt een aantal verplichte maatregelen.

De verplichte maatregelen zijn concreet:

1. Het bijhouden van een verwerkingsregister (register van verwerkingsactiviteiten).
2. Het bijhouden van een register van datalekken die zijn opgetreden.
3. Het bezitten van een toestemmingsverklaring betrokkenen.
4. Het aanstellen van een toezichthouder AVG (Functionaris Gegevensbescherming (FG)).
5. Privacy Verklaring.
6. Bestuursbesluiten rondom de AVG.
7. Beleid rondom continuïteit.

Bewustwording

Het is groot belang dat alle vrijwilligers die werken met persoonsgegevens de hoogte zijn van de nieuwe privacyregels. Zij moeten goed weten en kunnen inschatten wat de impact van de AVG is op hun taken, werkzaamheden en omgang met persoonsgebonden gegevens van vrijwilligers en welke aanpassingen nodig zijn om aan de AVG te voldoen. Daarom is dit AVG-protocol bekend bij alle vrijwilligers die werken met persoonsgegevens en zij kunnen dit dagelijks raadplegen.

1. Verwerkingsregister.

Algemene gegevens

Naam en contactgegevens van de stichting en de vertegenwoordiger van de stichting.

Naam : Rien Roelofse

Functie : Penningmeester

Email: : rien@stichtingbuitenzorg.nl

Categorie personen en persoonsgegevens

De stichting verwerkt de persoonsgegevens van de vrijwilligers. De bestanden van vrijwilligers en persoonsgegevens die gebruikt worden voor marketingdoeleinden worden apart geadministreerd.

De stichting verwerkt de volgende gegevens:

Algemene gegevens vrijwilligers

- NAW;
- Telefoonnummer; (is nodig om bij calamiteiten naaste betrokkenen te informeren)
- Emailadres; (is nodig om nieuwsbrieven te versturen met toestemming)
- Bij welke activiteiten de vrijwilliger actief is;
- Geboortedatum; (is nodig om een registratie voor verjaardag attenties te verzorgen)
- Datum gestart als vrijwilliger;

- Of er een VOG in ons bezit is;
- Of er een toestemmingsverklaring is voor foto publicatie;
- Of er een getekend vrijwilligers contract aanwezig is.
- Voor bestuursleden is een kopie van een recent geldig legitimatiebewijs aanwezig om ingeschreven te kunnen worden in het Handelsregister. In inschrijving vernietigen wij het ontvangen legitimatiebewijs.
- Nieuwsbrief ontvangen ja/nee

Grondslag van de verwerking

De AVG biedt zes grondslagen waarop verwerking van PG gebaseerd dient te zijn. Basing op één van de zes grondslagen volstaat. Het zijn deze grondslagen:

- 1) Nodig voor **overeenkomst** met betrokkene;
- 2) **Wettelijke verplichting**;
- 3) **Levensbelang** betrokkene;
- 4) Uitvoeren **overheidstaak**;
- 5) Uw **belang** weegt zwaarder dan belang betrokkene;
- 6) Betrokkene heeft **toestemming** gegeven.

Als wet verplicht om bepaalde PG te verwerken, dan moet dat ook.

Doel van verwerking

De algemene persoonsgegevens zijn nodig om uitvoering te geven aan de doelstelling van de stichting.

Bewaartermijn persoonsgegevens

Deze gegevens worden nadat een vrijwilliger definitief is gestopt met zijn of haar werkzaamheden verwijderd uit het actieve vrijwilligersbestand en overgezet naar het bestand gestopte vrijwilligers gegevens. De gegevens die bewaard worden zijn bestemd voor bijv. reünies en uitnodigingen voor recepties.

Delen gegevens met derden

Deze gegevens zijn bedoeld voor intern gebruik binnen de stichting. Deze kunnen worden geraadpleegd door de bestuursleden en de vrijwilligerscoördinator.

Gegevens worden niet gedeeld met derden.

Maatregelen tegen risico's

Het verwerken van persoonsgegevens van vrijwilligers brengt risico's met zich mee. Om te voorkomen dat onbevoegden toegang krijgen tot gevoelige gegevens van vrijwilligers zijn de elektronische/digitale bestanden opgeslagen in een met wachtwoorden en alleen voor strikt gereguleerde gebruikers toegankelijk. Dagelijks wordt een back up gemaakt van deze bestanden die eveneens alleen onder voorwaarden van wachtwoord voor strikt gereguleerde gebruikers toegankelijk.

De gegevens worden vastgelegd in een Excel bestand en via een beveiligde omgeving opgeslagen in mappen in Teams. Hosting geschiedt in Europa.

Rol Functionaris Gegevensbescherming

De stichting heeft geen externe Functionaris Gegevensbescherming aangesteld.

Bestuursbesluiten rondom de AVG.

Het bestuur heeft besloten dat het aangaan van een verwerkersovereenkomst bij de aantallen die wij laten drukken/verwerken een te zwaar middel is. Het ligt in de lijn der verwachting dat verwerkers niet zitten te wachten op kleine klanten zoals wij als ze ook nog de uitgebreide administratieve last hebben van het aangaan van een formele overeenkomst.

Het bestuur is ervan overtuigd dat wij werken met gerenommeerde partijen die zorgvuldig omgaan met de aan hen geleverde bestanden.

3. Datalekken.

Meldplicht.

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Organisaties, ook de stichting, die een ernstig datalek hebben, moeten dit sindsdien melden bij de Autoriteit Persoonsgegevens (AP) en soms ook aan de mensen van wie de gelekte gegevens zijn.

Beschrijving datalek

Een datalek is een lek waarbij persoonsgegevens *per ongeluk* bij iemand anders terecht komen dan de bedoeling is. Bijvoorbeeld:

- o Een verkeerd bezorgde brief;
- o Een e-mail aan de verkeerde ontvanger;
- o Een app aan de verkeerde ontvanger;
- o Een bestuurslid of vrijwilliger die in Teams mappen de gegevens van andere kan inzien waarvoor hij of zij geen machtiging heeft;
- o Een USB-stick met persoonsgegevens verloren/ gestolen;
- o Een laptop wordt gestolen;
- o Een inbraak in een databestand;
- o Een datalek in een smartphone;

Gebruikte termen in wet AVG

- o **Beveiligingsincident;** een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- o **Informatievoorziening;** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- o **Datalek;** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- o **Betrokkene;** de persoon van wie de persoonsgegevens zijn gelekt

Bij een datalek is sprake van een inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Onder een datalek valt dus niet alleen het vrijkomen (lekkens) van persoonsgegevens, maar ook (onzorgvuldige) vernietiging daarvan en andere vormen van onrechtmatige verwerking.

Registratie datalek

Om datalekken te registreren is er een formulier meldingsformulier datalekken. Deze wordt ingevuld door voorzitter en/of bestuurslid belast met privacy beleid. Het bestuurslid belast met privacy beleid controleert dit formulier 2x per jaar.

Melden datalek

Om datalekken te voorkomen zijn er afspraken.

Mocht zich onverhoopt een datalek voordoen, dan hangt van de ernst van het datalek af of er melding moet worden gedaan. De ernst wordt onder meer bepaald door het soort persoonsgegevens dat is gelekt. Een datalek moet volgens de wet bij de toezichthouder worden gemeld als dit:

“Leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens”.

In sommige gevallen moet de stichting het datalek ook melden aan de betrokkenen. Dit zijn de vrijwilligers van wie persoonsgegevens zijn verwerkt. Zij moeten worden geïnformeerd als een datalek *“waarschijnlijk ongunstige gevolgen zal hebben”* voor hun persoonlijke levenssfeer.

Beleidsregels

Eerder publiceerde het CBP (Collegebescherming persoonsgegevens, nu Autoriteit Persoonsgegevens, AP) al een concept van deze beleidsregels ter consultatie. Deze heette toen nog richtsnoeren meldplicht datalekken.

Boete

De Autoriteit Persoonsgegevens kan de stichting een boete geven als zij een datalek ten onrechte niet melden.

Maatregelen tegen datalekken.

De stichting neemt de volgende maatregelen waarmee het risico op een datalek door malware (bijvoorbeeld ransomware) verkleind wordt:

- Inzet goede beveiligingsmaatregelen zoals antivirussoftware, firewalls, anti-malwaresoftware, enz.
- Op tijd software-updates installeren;
- Geen verouderde (netwerk)protocollen gebruiken;
- Beveiligen computernetwerk en -systemen (scheiden).

Onze ICT-beheerder ziet hierop toe en voert tijdig de noodzakelijke handelingen uit.

De stichting maakt gebruik van moderne techniek (zie boven) om persoonsgegevens te beveiligen. Verder hebben we beschreven wie toegang heeft tot welke gegevens. De beveiliging van persoonsgegevens is binnen de stichting een blijvend punt van aandacht.

Praktische informatie bij malware

Om te voorkomen dat de stichting getroffen wordt door malware (gijzeling van bestanden die dan tegen betaling weer worden vrijgegeven), zijn maatregelen getroffen en zijn onze medewerkers zich bewust van deze gevaren.

Melden malware datalek

Als de stichting wordt getroffen door malware waarbij (mogelijk) persoonsgegevens betrokken zijn, dan onderzoeken we of de inbreuk leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Of dat er een aanzienlijke kans hierop is. Als dit zo blijkt te zijn, dan melden we dit bij de Autoriteit Persoonsgegevens.

De stichting gaat ook na of betrokkenen geïnformeerd moeten worden en zal dit doen als dit nodig blijkt. Dit hangt af van de aard van de gegevens welke gelekt zijn. Een deskundige, de ICT-beheerder eventueel ondersteunt door een externe deskundige, zal een analyse maken van o.a. logboekbestanden waarna besloten wordt wel/ niet te informeren.

4. Toestemmingsverklaring

Voor specifieke verwerking van PG heeft de stichting aparte toestemmingsverklaringen waarin toestemming gevraagd wordt om specifiek persoonsgebonden informatie (bijv. beeldmateriaal op de website) te gebruiken voor promotiedoeleinden. Voor alle toestemming geldt: Per gebeurtenis wordt vermeld hoe deze toestemming kan worden ingetrokken en wanneer deze informatie wordt verwijderd.

Eisen waar de toestemming aan moet voldoen.

De toestemmingsverklaring voldoet aan de volgende voorwaarden:

- ◇ De stichting heeft de toestemming vrij en niet onder druk verkregen. Een vrijwilliger of iemand uit onze doelgroep wordt niet benadeeld als hij/zij, de ouder/ verzorger geen toestemming geeft.
- ◇ De toestemming is ondubbelzinnig en duidelijk. Er is toestemming verleend. De stichting gaat niet uit van het principe 'wie zwijgt, stemt toe'.
- ◇ De stichting heeft toestemming gevraagd voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via beeldmateriaal op de sociale media, de Binnen- en/of Buitenpost verslag te doen van een activiteit.
- ◇ Het is voor vrijwilligers/ leden van onze doelgroep, ouders/ verzorgers gemakkelijk om de toestemmingsverklaring weer in te trekken. Onderaan de verklaring is de optie Intrekking toestemming aangegeven. Door de toestemmingsverklaring op te vragen, kunnen zij die optie invullen. (Zie toestemmingsverklaring).

** Foto's en video's waarbij vrijwilligers of leden van onze doelgroep herkenbaar in beeld zijn, zijn persoonsgegevens. Ook daar is toestemming voor nodig van de vrijwillige, lid van onze doelgroep, ouder/ verzorger. Zie ook hieronder 'Portretrecht'.*

Beveiliging & bescherming

De stichting heeft passende technische en organisatorische maatregelen getroffen om beeldmateriaal van vrijwilligers en leden van onze doelgroep leerlingen te beschermen. Deze maatregelen garanderen een dusdanig beveiligingsniveau dat beeldmateriaal niet in verkeerde handen terechtkomt. De stichting gebruikt geen Facebookpagina of vergelijkbare internetplatforms om beeldmateriaal te delen zonder toestemming van betrokkenen.

Portretrecht

Als op een foto of film e.d. een vrijwilliger of lid van een doelgroep te herkennen is, is er sprake van een "portret". Als er op een foto of film meerdere personen te zien zijn, heeft elk van hen het portretrecht. Het portretrecht is een beperking van het auteursrecht. De wet onderscheidt twee soorten portretten:

- Portretten die in opdracht van de geportretteerde zijn gemaakt.
- Portretten die niet in opdracht van geportretteerde zijn gemaakt.

De rechten die de afgebeelde persoon kan uitoefenen, is afhankelijk van het soort portret het betreft. Is er sprake van een portret dat gemaakt is in opdracht van de geportretteerde, dan mag de foto e.d. niet openbaar gemaakt worden zonder zijn toestemming. Het standaardvoorbeeld van een in opdracht gemaakt portret is een bruidsreportage. Het bruidspaar mag de fotograaf verbieden om de foto te publiceren of ten toon te stellen in zijn etalage.

Is het portret niet in opdracht van de geportretteerde gemaakt, bijv. een foto van Sinterklaasfeest in een van onze locaties gemaakt in opdracht van een krant, dan heeft de geportretteerde persoon minder rechten. De afgebeelde persoon kan zich dan alleen maar succesvol verzetten tegen publicatie (openbaarmaking), voor zover die persoon een redelijk belang heeft om zich daartegen te verzetten. De vrijwilliger of lid van onze doelgroep heeft dus in beginsel geen recht om de publicatie van foto's waarop hij te herkennen is tegen te houden.

Auteursrecht.

Het is een misverstand dat teksten en foto's die op internet staan, vrijelijk gekopieerd en gebruikt zouden mogen worden. Dat is beslist niet het geval, zelfs niet met bronvermelding!

5. Functionaris Gegevensbescherming (FG)

Met ingang van 25 mei 2018 geldt de Algemene verordening Gegevensbescherming (AVG). Vanaf dit moment zijn organisaties verplicht een functionaris voor de Gegevensbescherming (FG) aan te stellen.

Voor kleine organisaties als onze stichting is zo'n functionaris niet verplicht, vooral ook omdat wij geen bijzondere persoonsgegevens opslaan en/of grootschalig gegevens verwerken.

De privacy taak is voor onze stichting belegd bij het bestuurslid algemene zaken van onze stichting.

AVG en bewaartermijnen

De Algemene verordening Gegevensbescherming (AVG) brengt geen veranderingen met zich mee voor de persoonsgegevens van vrijwilligers die de stichting mag bewaren in het dossier. Ook verandert er niets voor de bewaartermijn en het recht op inzage voor de vrijwilliger in het dossier.

Bewaartermijn

De stichting hanteert de volgende bewaartermijnen:

- ◇ Een vrijwilligersdossier: 2 jaar nadat de vrijwilliger definitief is uitgeschreven. In sommige situaties geldt een langere bewaartermijn.

Adresgegevens voor reünies

De stichting mag adresgegevens van oud-vrijwilliger bewaren voor bijv. het organiseren van reünies. De stichting heeft toestemming (zie toestemmingsverklaring) om die gegevens voor dat doel te gebruiken.

Inhoud (digitale) dossiers

De stichting bewaart verschillende gegevens over een vrijwilliger in het (digitale) vrijwilligersdossier. Dit dossier bestaat uit administratieve gegevens en informatie die nodig zijn voor het kunnen uitvoeren van de activiteiten zoals omschreven in de statuten van de stichting. Dit dossier bevat de volgende gegevens:

- ◇ NAW-gegevens;
- ◇ Gegevens over in- en uitschrijving;
- ◇ Geboortedatum;
- ◇ Geslacht;
- ◇ Toestemming foto
- ◇ Verklaring omtrent Gedrag (VOG)
- ◇ Telefoonnummer
- ◇ Emailadres
- ◇ Betrokken bij welke activiteit

Nieuwe Europese privacyregels

Onder de AVG wordt de bescherming van persoonsgegevens van kinderen nog belangrijker. De stichting moet niet alleen de regels voor toestemming en beveiliging naleven, maar moet dat ook kunnen aantonen.

Toestemming en beveiliging zijn zoals al beschreven twee belangrijke voorwaarden. De AVG bevat nog meer rechten en verplichtingen bij de verwerking van persoonsgegevens. De stichting neemt deze uiteraard in acht.

Privacy by design

De stichting besteedt aandacht aan:

1. Privacy verhogende maatregelen: bij het gebruik van producten en diensten zorgt de stichting ervoor dat persoonsgegevens goed worden beschermd.
2. Dataminimalisatie: de stichting verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen *die gegevens die noodzakelijk* zijn voor het *doel* van de verwerking.
3. Bewaartermijn: de stichting bewaart de gegevens niet langer dan nodig (zie bewaartermijn).
4. Privacy risico's van een product of dienst bij ingebruikname daarvan, zodat voorkomen wordt dat er later noodzakelijke aanpassingen nodig zijn die zeer tijdrovend en kostbaar zijn.

Privacy by default

De stichting neemt technische en organisatorische maatregelen die ervoor te zorgen dat alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat de stichting wil bereiken.

Privacyverklaring

De stichting legt gegevens vast zoals naam, adres, woonplaats, emailadres en overige gegevens die noodzakelijk zijn voor de uitvoering van de activiteiten zoals omschreven in de statuten en voor de uitvoering van het donateurschap of de verwerking van een eenmalige gift. Wij verstrekken uw gegevens uitsluitend aan partijen die diensten voor onze stichting uitvoeren zoals drukkers voor het afdrucken van etiketten en banken voor de verwerking van incassomachtigingen, en alleen die gegevens die voor de betreffende verwerking noodzakelijk zijn. Alle aan ons toevertrouwde informatie wordt door ons en door onze leverancier vertrouwelijk behandeld. Uw e-mailadres wordt uitsluitend gebruikt om informatie te sturen die onze stichting betreffen zoals nieuwsbrieven.

Uw gegevens worden alleen gebruikt voor de doeleinden waarvoor ze zijn verkregen.

U kunt zich te allen tijde afmelden als donateur. Stuur daarvoor een mail aan info@stichtingbuitenzorg.nl

Ook adreswijzigingen en andere wijzigingen kunt u doorgeven aan ons secretariaat info@stichtingbuitenzorg.nl

Relevante websites

Autoriteit Persoonsgegevens [Algemeen](#).

Autoriteit Persoonsgegevens [Dossier AVG](#)

Autoriteit Persoonsgegevens [Privacywetgeving](#)

Autoriteit Persoonsgegevens [Persoonsgegevens](#)

Autoriteit Persoonsgegevens [Verantwoordingsplicht](#)