



AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat Activerende zorgcoach Foliant het AVG-programma geheel of gedeeltelijk heeft doorlopen. Activerende zorgcoach Foliant verklaart hiermee dat de inspanningen zijn verricht zoals die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Indien niet alle programmaonderdelen zijn afgewerkt en de verklaring toch wordt aangevraagd, dan is geen volledige invulling gegeven aan de eisen van de wetgever. De Stichting AVG voor Verenigingen adviseert de openstaande punten alsnog zo snel mogelijk af te werken en in elk geval in het programma een aantekening te maken wanneer dit zal gebeuren.

In de hierna volgende verklaring staan alle onderdelen/stappen die Activerende zorgcoach Foliant heeft doorlopen om te voldoen aan de AVG-wetgeving. Per onderdeel is duidelijk aangegeven welke gegevens en onderdelen van de wet van toepassing zijn en hoe daar aan voldaan is. Waar nodig is additionele informatie verstrekt ter verduidelijking van de situatie.

Activerende zorgcoach Foliant begrijpt dat AVG-wetgeving continu van toepassing is en dat wij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft Activerende zorgcoach Foliant kennis over de materie ontvangen die door de AVG wordt geraakt, en verklaart zelf naar eer en geweten aan de wet te voldoen. De onderdelen van de zelfverklaring door Activerende zorgcoach Foliant zijn te vinden op de volgende pagina('s) van deze verklaring.

Aldus opgemaakt te Gorinchem,

d.d. 21-6-2021,

door Stichting AVG voor Verenigingen

gevestigd aan de Stephensonweg 14 te Gorinchem.

2.1 Inventarisatie persoonsgegevens.

Geef hieronder aan welke persoonsgegevens binnen de organisatie gebruikt worden.

Gewone persoonsgegevens

- Naam/ voorletters/ tussenvoegsel
- Titels
- Adres
- Postcode
- Plaats
- Provincie
- Land
- Woonplaats
- Telefoonnummer
- Faxnummer
- E-mailadres
- Website
- Geslacht
- Geboortedatum
- Geboorteplaats
- Overlijdensdatum
- Burgerlijke staat
- LinkedIn
- Facebook
- Twitter
- Werkzaam bij organisatie
- Bankrekeningnummer
- Inloggegevens (gebruikersnaam/wachtwoord)
- Voertuig kentekenplaat
- Salarisgegevens Salarisgegevens worden niet gezien als bijzondere gegevens.

Andere gewone persoonsgegevens:

Bijzondere persoonsgegevens

- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuiging
- Lidmaatschap van een vakbond
- Genetische of biometrische gegevens met het oog op unieke identificatie
- Gegevens over gezondheid
- Gegevens over seksueel gedrag of seksuele gerichtheid
- Strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
- Kopie identiteitsbewijs/paspoort, zonder voorlegger gekopieerd
- BSN-nummer Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald. Dit geldt bijvoorbeeld voor werkgevers, zorgverleners, zoals huisartsen, apotheken en zorgverzekeraars. Ook in het onderwijs en kinderopvang wordt het BSN gebruikt.

Aantekeningen bijzondere persoonsgegevens:

3.1 Inventarisatie doelbinding.

Grondslag:

Je moet een goede reden hebben om persoonsgegevens te mogen verwerken. De juridische naam voor die redenen is grondslagen. U heeft dus een grondslag nodig om persoonsgegevens te mogen verwerken. In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

U heeft toestemming van de persoon om wie het gaat,

Het is noodzakelijk om gegevens te verwerken,

om een overeenkomst uit te voeren,

omdat u dit wettelijk verplicht bent,

om vitale belangen te beschermen,

om een taak van algemeen belang of openbaar gezag uit te oefenen.

Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

Voorbeelden van grondslagen zijn:

Toestemming = ondertekening van een toestemmingsformulier of een inschrijving door middel van een opt-in voor een nieuwsbrief,

Overeenkomst = je hebt deze persoonsgegevens nodig voor het uitvoeren van een overeenkomst (b.v. een koopcontract of een lidmaatschapsovereenkomst),

Gerechtvaardigd belang = bestaande klanten na een aankoop te informeren over soortgelijke, eigen producten of diensten.

Doelbinding:

Welke persoonsgegevens verwerk je, met welk doel en heb je ze daar ook voor gekregen (grondslag)? Dat noemen we 'doelbinding'. Het is belangrijk dat je persoonsgegevens alleen verwerkt (dus opslaat en gebruikt) voor de doeleinden waarvoor je deze hebt verkregen. In de doelbinding beschrijf je dus welke gegevens, met welke grondslag en wat je met die gegevens doet.

Voor de inventarisatie van de vormen van doelbinding binnen de organisatie hebben wij onderstaand schema gemaakt. Voor doelbindingen die veel voorkomen, hebben wij het schema al ingevuld en die kun je dus zo aanvinken. Komen er binnen je organisatie nog andere doelbindingen voor, dan kun je deze in de open vorm noteren bij 3.3.

Bewaartermijn:

Het uitgangspunt is dat je persoonsgegevens niet langer mag bewaren dan noodzakelijk. Wat noodzakelijk is hangt af van de situatie. Dit staat niet concreet beschreven in de AVG en dus moet je bepalen wat in jouw situatie passend is.

Wel zijn er andere wettelijke termijnen waar u zich aan moet houden. Bijvoorbeeld op grond van belastingwetgeving of de Archiefwet. Zo moet je voor de belastingdienst je administratie 7 jaar bewaren.

LET OP: Je bent wettelijk verplicht zo min mogelijk persoonsgegevens te verwerken. Vraag dus alleen de gegevens die je echt nodig hebt voor het goed functioneren van je organisatie.

(N = Naam, A = Adres, W = Woonplaats, T = Telefoon, E = e-mailadres)

Klant of leverancier

Persoonsgegevens: NAWTE.

Grondslag: Opdracht of contract.

Verwerkingen: Administratie, bevestiging, uitlevering.

Verwerkt door: Afdeling administratie, afdeling sales en afdeling inkoop.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

Beschrijf hieronder kort uw situatie:

Klant en BSN

Organisaties buiten de overheid mogen het BSN (burger-servicenummer) alleen gebruiken als dat volgens de wet is toegestaan. Anders mag het niet! Het is toegestaan voor bijvoorbeeld werkgevers, zorgverleners, zoals huisartsen en apotheken en ook voor zorgverzekeraars. Ook in het onderwijs wordt het BSN gebruikt. Hier heet het ook wel onderwijsnummer of persoonsgebonden nummer. Organisaties kunnen niet onder het verbod uitkomen door mensen toestemming te vragen voor het gebruik van hun BSN!

Persoonsgegevens: NAWTE + BSN.

Grondslag: Overeenkomst met handtekening op papier.

Verwerkingen: Interactie met de overheid in het belang van (en met toestemming van) de klant.

Verwerkt door: Afdeling administratie.

Bewaartermijn: Gedurende de looptijd van de overeenkomst.

Beschrijf hieronder kort uw situatie:

VvE-leden en -gebruikers

Het bestuur van de VvE dient op grond van het reglement ex artikel 5:112 BW een register bij te houden van eigenaars en een register van gebruikers. In dit register zijn persoonsgegevens opgenomen.

Persoonsgegevens: NAWTE + bankgegevens + kentekengegevens.

Grondslag: Akte van splitsing en het reglement ex artikel 5:112 BW.

Verwerkingen: Beheeractiviteiten van de VvE in de breedste zin van het woord in het belang van (en met toestemming van) de (gezamenlijke) eigenaars.

Verwerkt door: Bestuur en beheerder.

Bewaartermijn: Gedurende lidmaatschap of gebruik en 12 maanden daarna en voorts alleen in de financiële administratie voor maximaal 7 jaar.

Beschrijf hieronder kort uw situatie:

Aanmelden voor nieuwsbrief

Persoonsgegevens: Naam en e-mailadres.

Grondslag: Aanmelding voor nieuwsbrief (formulier op de website).

Verwerkingen: Informatie verstrekking in de vorm van nieuwsbrieven.

Verwerkt door: Afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men aangemeld is.

Beschrijf hieronder kort uw situatie:

Prospect, stakeholder-/lobbycontacten en geïnteresseerde

Persoonsgegevens: NAWTE.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Informatieverstrekking in de vorm van nieuwsbrieven of gerichte contacten.

Verwerkt door: Afdeling communicatie, directie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men contact heeft.

Beschrijf hieronder kort uw situatie:

Stakeholder-/lobbycontacten met politieke voorkeur

Persoonsgegevens: NAWTE + politieke voorkeur.

Grondslag: Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.

Verwerkingen: Persoonlijke contacten en nieuwsvoorziening.

Verwerkt door: Afdeling communicatie, directie.

Bewaartermijn: Gedurende de periode dat men contact heeft.

Beschrijf hieronder kort uw situatie:

Medewerkers

Persoonsgegevens: NAWTE + geboortedatum, kopie ID en bankgegevens.

Grondslag: Arbeidsovereenkomst.

Verwerkingen: Salariëring.

Verwerkt door: HRM-afdeling.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

In plaats van medewerkers werk ik met collega zzp-ers of mkb waarbij ik gebruik maak van hun gegevens met toestemming van de betrokkenen.

Medewerkersfoto's op de website

Persoonsgegevens: Naam + foto.

Grondslag: Aanvullende personeelsovereenkomst.

Verwerkingen: Medewerkersfoto's op website.

Verwerkt door: Administratie, afdeling communicatie.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

We werken samen met andere midden- en klein bedrijven in de vorm van zzp-ers.

De foto of het logo wordt gedeeld op mijn website met toestemming van de betrokken organisatie of persoon.

Vrijwilligers

Persoonsgegevens: NAWTE.

Grondslag: Vrijwilligersovereenkomst.

Verwerkingen: Informatieverstrekking.

Verwerkt door: Afdeling communicatie, vakkennisafdelingen en/of relatie beheerder.

Bewaartermijn: Gedurende de periode dat men een contract heeft.

Beschrijf hieronder kort uw situatie:

Direct marketing (alleen bellen of papier)

Persoonsgegevens: NAWTE.

Grondslag: Geen overeenkomst nodig.

Verwerkingen: Toesturen van (of bellen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

Beschrijf hieronder kort uw situatie:

Wanneer er een contactformulier ingevuld wordt via mijn website , of wanneer er gebeld wordt, neem ik contact op met de betrokkenen en geef ik indien gewenst informatie over mijn bedrijf.

Digitale direct marketing (e-mail, facebook, LinkedIn, fax, SMS etc.)

Persoonsgegevens: NAWTE.

Grondslag: Digitale toestemming vooraf, b.v. bij aanvragen van informatie of inschrijven voor een nieuwsbrief.

Verwerkingen: Digitaal toesturen van (of benaderen over) informatie over de organisatie en/of producten/diensten.

Verwerkt door: Afdeling marketing/communicatie.

Bewaartermijn: Gedurende de periode dat men gezien wordt als prospect voor de organisatie of haar diensten/producten.

Beschrijf hieronder kort uw situatie:

Voor mijn bedrijf heb ik een facebook pagina en een website.

3.3 Beschrijving van extra doelbinding.

Als je meer persoonsgegevens, verwerkingen en/of overeenkomsten hebt dan bij 3.1 beschreven, voeg deze dan hieronder toe. Voeg de extra beschrijving over doelen en doelbinding hieronder toe zodat we die kunnen opnemen in de AVG-verklaring.

Binnen de organisatie is er veel contact en afstemming met verschillende beschikingsstellers binnen gemeentes, onderaannemers, behandelaars.

Gegevens worden via een beveiligd systeem met elkaar gedeeld. (KIS , Mextra, Vecozo, VNG, beveiligd mailsysteem filecap)

4.1 Privacy policy vindbaar, verwijzing in documenten.

De privacy policy van de organisatie moet voor iedereen waarvan je persoonsgegevens verwerkt vindbaar zijn. Het eenvoudigste is om deze op de website van de organisatie te zetten en op elke pagina (onderaan) een link hier naartoe te leggen.

- Wij als organisatie hebben onze privacy policy zichtbaar gemaakt op onze website.
- Wij als organisatie hebben onze privacy policy niet vindbaar gemaakt op onze website.

Beschrijf hieronder kort uw situatie:

In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

- Wij als organisatie verwijzen in al onze documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan naar onze privacy policy op de website van de organisatie.
- Wij als organisatie verwijzen in documenten (contract, overeenkomst, aanmeldingsformulier, etc.) waarin persoonsgegevens staan niet naar onze privacy policy op de website van de organisatie.

Beschrijf hieronder kort uw situatie:

5.1 Werken met verwerkersovereenkomst.

Als organisatie mag je persoonsgegevens niet doorgeven aan een andere partij welke ten behoeve van jou persoonsgegevens verwerkt zonder een verwerkersovereenkomst. In een verwerkersovereenkomst spreek je af wat de ander met de gegevens mag doen én ook vooral wat niet.

- Wij als organisatie verklaren dat wij nooit persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor we ze hebben gekregen.
- Wij als organisatie verklaren dat wij ook persoonsgegevens doorgeven aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten.
- Wij als organisatie verklaren dat wij geen persoonsgegevens doorgeven aan andere partijen.

Beschrijf hieronder kort uw situatie:

6.1 Toegangsbeveiliging.

Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kun je een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat je altijd minimaal één keer een wachtwoord moet weten voordat je de persoonsgegevens van jouw organisatie kunt inzien of bewerken.

- Wij als organisatie hebben persoonsgegevens altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- Wij als organisatie hebben persoonsgegevens niet altijd opgeslagen achter de beveiliging van minimaal een gebruikersnaam en een wachtwoord.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen toegangsbeveiliging.

Beschrijf hieronder kort uw situatie:

Er wordt gebruik gemaakt van een cliënt volgsysteem (Mextra, VNG en KIS)

7.1 Software en antivirussoftware up-to-date.

Om systemen zo veilig mogelijk te laten zijn, moet je ze up-to-date houden. Dit doe je door het aanzetten van het automatisch ophalen en installeren van updates van de software. Zorg ook voor goede antivirussoftware. Zorg ervoor dat alle software ingesteld is op het automatisch ophalen en uitvoeren van updates. Maak goede afspraken met al je softwareleveranciers.

- Wij als organisatie hebben de persoonsgegevens alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- Wij als organisatie hebben de persoonsgegevens niet alleen opgeslagen op computers/servers met beveiligingssoftware waarbij zowel de beveiligingssoftware als het besturingssysteem ingesteld zijn om automatisch updates op te halen en te installeren.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen software updates.

Beschrijf hieronder kort uw situatie:

8.1 Opslaan alleen binnen de EU.

Binnen de EU is het niveau van gegevensbescherming gelijk. Dat komt omdat alle EU-lidstaten moeten voldoen aan de AVG. Als je persoonsgegevens verwerkt buiten de EU, bijvoorbeeld door deze te laten verwerken door een partij buiten de EU of er een passend beschermingsniveau bestaat voor dat land, bijvoorbeeld door een adequaatheidsbesluit van de Europese Commissie.

De wetgever is dus extra streng als je persoonsgegevens wilt verwerken/opslaan buiten de EU. Als je dat toch zou willen, dan moet er heel veel geregeld worden bovenop de normale AVG-verplichtingen. Dus check of je dienstverlener (drukker, verspreider, enz.) de toevertrouwde persoonsgegevens binnen de EU opslaat.

Het is dus het makkelijkste om persoonsgegevens alleen te verwerken binnen de EU, dit raden wij daarom ook sterk aan.

- Wij als organisatie verklaren dat wij nooit persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.
- Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU.

Beschrijf hieronder kort uw situatie:

9.1 Data back-up.

Om de persoonsgegevens te beschermen tegen het verlies of diefstal moet je back-ups maken. Het is noodzakelijk om dat regelmatig te doen. Zorg ervoor dat deze back-up veilig wordt opgeborgen.

- Wij als organisatie hebben de opgeslagen persoonsgegevens beveiligd met een back-up.
- Wij als organisatie hebben de persoonsgegevens niet beveiligd met een back-up.
- Wij als organisatie hebben geen persoonsgegevens elektronisch opgeslagen en hebben daarom geen back-up.

Beschrijf hieronder kort uw situatie:

10.1 Geautoriseerde medewerkers.

Via autorisatie regel je wie binnen de organisatie welke persoonsgegevens mag verwerken.

- In onze organisatie hebben alleen geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.
- In onze organisatie hebben ook niet geautoriseerde personen toegang tot de persoonsgegevens van de organisatie.

Beschrijf hieronder kort hoe jullie de autorisatie geregeld hebben:

Bij Activerende Zorgcoach Foliant heeft iedere zzp-er een persoonlijke gebruikersnaam en wachtwoord om bij Mextra te kunnen inloggen bij de gekoppelde zorgvrager. Ik autoriseer deze collega toegang te krijgen tot de relevante gegevens die betrekking hebben op de zorgvraag van de zorgvrager om de ondersteuning op de juiste wijze te kunnen verlenen en aan de gestelde doelen te werken, zodat zij niet bij andere zorgvragers in het dossier kunnen. Ik als eigenaar ben beheerder van het systeem zodat ik het overzicht kan behouden en ben ook de enige die toegang heeft tot alle dossiers e.d. die in het systeem staan. De zorgvrager kan ook in het systeem mbt hun eigen dossier ivm de transparantie. Ook zij hebben hiervoor een persoonlijk wachtwoord en gebruikersnaam voor ontvangen.

Onderstaande vragen zijn alleen ter bewustwording en hoeven niet precies ingevuld te worden!

Wij als organisatie hebben 5 personen geautoriseerd om de persoonsgegevens van de organisatie in te zien en te verwerken indien dit nodig is voor de uitoefening van hun functie.

Wij als organisatie hebben van 100 personen de persoonsgegevens geregistreerd.

11.1 Vernietigen persoonsgegevens.

Geef hieronder aan dat je organisatie alle persoonsgegevens vernietigt door bijvoorbeeld een regel te wissen in Excel en/of het versnipperen van een aanmeldingsformulier als er geen overeenkomst meer is. Persoonsgegevens mogen niet langer worden bewaard dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt. Dus: na beëindiging van een overeenkomst worden de persoonsgegevens van die persoon vernietigd.

Wijs aan wie verantwoordelijk is voor het vernietigen van persoonsgegevens of de controle op de vernietiging.

NB: Verscheuren en weggooien is onvoldoende. Schaf daarom een versnipperaar aan.

Let op: In de financiële administratie mogen (of eigenlijk: moeten!) deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar.

- Wij als organisatie verklaren dat wij alle persoonsgegevens vernietigen (na de bewaartermijn) als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.
- Wij als organisatie verklaren dat wij geen persoonsgegevens vernietigen als de overeenkomst op grond waarvan ze verkregen zijn verlopen is of de toestemming is ingetrokken.

Beschrijf hieronder kort uw situatie:

behalve wanneer het gaat om de financiële administratie

12.1 Toestemming voor direct marketing en bij minderjarigheid.

Bij direct marketing.

De wetgever maakt onderscheid tussen gewone direct marketing (bellen en post sturen) of digitale marketing (via e-mail, fax, Facebook, LinkedIn of sms). Doordat gewone direct marketing een organisatie bij de verspreiding veel geld kost zal dat altijd beperkt blijven. Juist digitale marketing is nagenoeg gratis en kan daardoor heel veel toegepast worden met alle gevolgen van dien.

Op grond van de Telecommunicatiewet mag je bestaande klanten benaderen via digitale direct marketing zonder toestemming (maar met een opt-out).

- Wij als organisatie vragen vooraf altijd toestemming voordat we iemand benaderen via digitale direct marketing.
- Wij als organisatie vragen vooraf geen toestemming voordat we iemand benaderen via digitale direct marketing.
- Wij als organisatie maken geen gebruik van digitale direct marketing.

Beschrijf hieronder kort uw situatie:

Als organisatie vraag ik altijd eerst toestemming om bijv. een foto of tekst op mijn website/facebook te mogen plaatsen. Hiervoor heb ik een schriftelijke toestemmingsverklaring. Ook wanneer er meerdere personen op 1 foto staan en zij de foto graag willen ontvangen voor eigen gebruik wordt er eerst toestemming gevraagd aan de andere personen die ook op de foto staan.

Bij minderjarigheid (jonger dan 16 jaar).

Als je persoonsgegevens online verwerkt van personen jonger dan 16 jaar via bijvoorbeeld een app, online game, webwinkel of via sociale media, dan moet je daarvoor altijd schriftelijk/elektronisch een toestemming hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hieronder aan dat je organisatie dat ook altijd zo doet.

- Wij als organisatie verklaren dat wij alleen online persoonsgegevens van minderjarigen verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media als daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- Wij als organisatie verklaren dat wij persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media zonder dat daarvoor schriftelijke toestemming is gegeven door de ouder, verzorger of wettelijke vertegenwoordiger.
- Wij als organisatie verklaren dat wij geen persoonsgegevens van minderjarigen online verwerken bijvoorbeeld een app, online game, webwinkel of via sociale media.

Beschrijf hieronder kort uw situatie:

Als organisatie vraag ik altijd eerst toestemming om bijv. een foto of tekst op mijn website/facebook te mogen plaatsen. Hiervoor heb ik een schriftelijke toestemmingsverklaring. Ook wanneer er meerdere personen op 1 foto staan en zij de foto graag willen ontvangen voor eigen gebruik, wordt er eerst toestemming gevraagd aan de andere personen die ook op de foto staan. Bij minderjarigen vragen wij altijd toestemming aan de wettelijk verantwoordelijke van de zorgvrager.

13.1 Papieren documenten en beveiliging.

Als persoonsgegevens ook vastliggen op papier (denk aan contracten), dan moeten die papieren met persoonsgegevens achter slot en grendel zijn opgeslagen. Praktisch: bewaar dus alle papieren met persoonsgegevens in een kast die je steeds op slot doet. Alleen personen die voor hun werk voor de organisatie daarvoor toestemming hebben, mogen in die kast komen.

- Wij als organisatie hebben papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- Wij als organisatie hebben niet alle papieren documenten waarop de persoonsgegevens staan, opgeslagen achter slot en grendel.
- Wij als organisatie hebben geen papieren documenten waarop de persoonsgegevens staan.

Beschrijf hieronder kort uw situatie:

De papieren documenten zijn opgeslagen in een afgesloten dossierkast, waar alleen ik als eigenaar toegang toe heb.

De sleutel wordt op een veilige plaats opgeborgen waar ik alleen toegang toe heb

14.1 Datalekken.

Iedereen in de organisatie moet op de hoogte zijn wat een datalek is en wat je eraan moet doen. Geef aan wat voor jullie van toepassing is:

- Binnen onze organisatie is iedereen op de hoogte van wat een datalek is. Ook is bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.
- Binnen onze organisatie is niet iedereen op de hoogte van wat een datalek is. Ook is niet bekend waar dit intern gemeld moet worden zodat wij als organisatie adequaat het datalek kunnen afhandelen en documenteren.

Beschrijf hieronder kort hoe jullie met datalekken omgaan:

Bij Activerende Zorgcoach Foliant zijn er per geen bestanden meer op de laptop opgeslagen maar staat alles in het beveiligde cliëntvolgsysteem. Er wordt nu ook geen gebruik gemaakt van een usb-stick omdat deze niet beveiligd zijn en de privacy bij Activerende Zorgcoach Foliant hoog in het vaandel staat. Besproken is dat wanneer er een data lek zal ontstaan, er altijd contact opgenomen wordt met mij als eigenaar. Ik zal dan een melding maken bij het beveiligde systeem. Ik maak bij mailverkeer gebruik van BCC, wanneer ik dit niet doe krijg ik de melding dat ik het in CC heb gezet en pas deze dan aan naar BCC indien gewenst.

15.1 Medewerkers geïnstrueerd

Wij hebben onze medewerkers als volgt geïnstrueerd:

- Alle medewerkers hebben de video van de Stichting AVG bekeken.
- We hebben het onderwerp privacy bescherming in alle afdelingsoverleggen besproken.
- We hebben uitlegposters opgehangen.
- We hebben alle medewerkers een brief gestuurd met uitleg en instructie.
- We hebben met alle medewerkers een workshop over privacy bescherming gevolgd.
- We hebben een nieuwsbrief voor alle medewerkers waarin we regelmatig aandacht besteden aan privacy bescherming.
- Onze directeur/voorzitter heeft alle medewerkers opgeroepen extra aandacht te besteden aan privacy bescherming.

Hieronder is ruimte om te beschrijven hoe jullie de medewerkers geïnstrueerd hebben:

Tijdens intervisie hebben we het AVG beleid besproken met de collega zzp-ers die ik inzet op aanvraag. De instructie video van de stichting AVG getoond en van daaruit zijn de onderwerpen besproken en hebben zij de uitlegposter ontvangen.

16.3 Afronding.

Naam organisatie: Activerende zorgcoach Foliant
Plaats: Dongen
Datum: 21-6-2021

De AVG-verklaring is een automatische samenvatting van alle vragen en antwoorden in het stappenplan. De AVG-verklaring is geen juridisch document maar een verklaring waarin je zelf verklaart dat je alle inspanningen hebt gepleegd om aan de Algemene Verordening Gegevensbescherming te voldoen. Wij zien in de praktijk dat sommige gebruikers de AVG-verklaring regelmatig opvragen en gebruiken als een todo lijst. Je kunt de AVG-verklaring zo vaak opvragen als je wilt.