

AVG verklaring



Angsthelden

Uitgegeven op 14-2-2024



Geldig tot 14-5-2024

De bescherming van persoonlijke gegevens is geen eenmalige zaak.

Ook al heb je het eenmalig goed ingericht, de wet vereist dat je met een actueel document kunt aantonen dat je voldoet aan de AVG. De Autoriteit Persoonsgegevens (AP) controleert dat steekproefsgewijs.

Deze AVG-verklaring laat zien dat je alle verplichtingen vanuit de wet AVG hebt uitgevoerd (mits je alle onderdelen hebt ingevoerd). Als er iets verandert in jouw organisatie kun je de stappen opnieuw bekijken en eventueel aanpassen. Daarna vraag je de AVG-verklaring opnieuw op door op de "Verklaring Aanmaken" knop te klikken.

Ook ontvang je elk kwartaal automatisch een nieuwe AVG-verklaring. Bewaar deze digitaal of print hem uit. Zo ben je altijd up-to-date!

AVG verklaring

Hierbij verklaart de Stichting AVG voor Verenigingen dat Angsthelden het AVG-programma geheel of gedeeltelijk heeft doorlopen. Angsthelden 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 Angsthelden 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.

Angsthelden begrijpt dat AVG-wetgeving continu van toepassing is en dat zij regelmatig de gegevens moeten controleren en updaten.

Met het volledig doorlopen van het AVG-programma van de Stichting AVG voor Verenigingen heeft Angsthelden 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 Angsthelden zijn te vinden op de volgende pagina(s) van deze verklaring.

Aldus opgemaakt te Den Haag,

d.d. 14-2-2024,

door Stichting AVG voor Verenigingen

gevestigd aan de Doctor Kuiperstraat 10 te Den Haag.

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

Andere gewone persoonsgegevens

Uw situatie:

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

Aantekeningen bijzondere persoonsgegevens

Angsthelden verzameld persoonsgegevens van mensen die kampen met een vorm van vliegangst

Persoonsgegevens die Angsthelden verzameld:

- In welke mate en in welke vorm de mensen last hebben van vliegangst;
- Of er sprake is van andere fysieke en/of mentale klachten;
- Medicatiegebruik.

Deze gegevens worden verzameld en opgeslagen in het CRM systeem van Teamleader. Ter beveiliging maakt Teamleader gebruik van een SSL-versleutelde verbinding bij al het internetverkeer. Om de data op te slaan wordt er gebruik gemaakt van Amazon Web Services (AWS). Deze servers ondergaan periodieke evaluatie zodat ze aan de nieuwste standaarden voldoen. Het systeem van Teamleader voldoet aan de

slaan wordt er gebruik gemaakt van Amazon Web Services (AWS). Deze servers ondergaan periodieke evaluaties zodat ze aan de nieuwste standaarden voldoen. Het systeem van Teamleader voldoet aan de volgende veiligheidsnormen:

- ISO27001;
- SOC 1 en SOC2/SSAE 16/ISAE 3402 (voorheen SAS 70 Type II);
- PCI Level 1;
- C5 Operational Security;
- ENS High;
- IT-Grundschutz.

Zodra een afspraak definitief ingepland is, wordt het gespreksverslag van de cliënt in Google Agenda gezet met daarbij het mailadres en het telefoonnummer van de cliënt. Deze gegevens zijn enkel toegankelijk voor de vliegangst trainers en het secretariaat. Google heeft haar data beveiligd opgeslagen in haar data centers.

Verder verzameld Angsthelden extra persoonsgegevens rondom begeleide vluchten:

-Een kopie van de voor- en achterkant van een geldig paspoort ten behoeve van het boeken van vluchten

-Een registratieformulier waarbij de volgende gegevens verzameld worden:

- Voornaam (of voornamen) als in paspoort;
- Achternaam als in paspoort;
- Contactpersoon en contactgegevens die we kunnen bereiken in geval van nood;
- Medicatiegebruik;
- Fysieke beperkingen;
- Mentale problemen;
- Of de cliënt fit-to-fly is.

Deze gegevens worden opgeslagen in Google Drive en zijn enkel toegankelijk voor de vliegangst trainers en het secretariaat. Google heeft haar data beveiligd opgeslagen in haar data centers.

3.1 Inventarisatie doelbinding

Grondslag

Je moet een goede reden hebben om persoonsgegevens te mogen verwerken. De juridische naam voor die redenen is grondslagen. Je hebt 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 je je 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

Angsthelden verwerkt NAWTE gegevens ten behoeve van het maken van afspraken, facturatie en het boeken van vluchten.

☐ 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

☐ 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

☐ 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

☐ 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

☐ 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

☒ 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

Medewerker in loondienst betreft: Mw.J. van der Goes. Angsthelden verwerkt NAWTE gegevens + geboortedatum, kopie ID en bankgegevens. Deze gegevens worden in de beveiligde omgeving van Google Drive bewaard. Daarnaast huurt Angsthelden freelance trainers in voor het geven van vliegangst trainingen. Ook van hen verwerkt Angsthelden NAWTE gegevens + geboortedatum, kopie ID en bankgegevens. Deze gegevens worden in de beveiligde omgeving van Google Drive bewaard.

☒ 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

Op <https://angsthelden.com/ons-team/> en staan de namen + foto's van onze medewerker en onze freelancers. Angsthelden heeft binnen de Wordpress omgeving maatregelen genomen ter bescherming van de content + foto's op de site.

☐ 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

☐ 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

☐ 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.

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.

Toelichting:

Uw situatie:

4.1 Privacy policy vindbaar, verwijzing in documenten

De privacy policy van de vereniging moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de vereniging te zetten en op elke pagina (onderaan) een link hier naar toe 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:

Op onze website <https://www.angsthelden.com/privacyverklaring> is ons privacy beleid terug te vinden.

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:

Wij verwijzen in onze mailwisselingen en afspraakbevestigingen naar ons privacy policy.

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:

Onderstaande partijen beschikken over een verwerkersovereenkomst. Tussenhaakjes is het bedrijfstype beschreven:

- Verdoorn Adviesgroep (accountant)
- Exact Online (software financiën)
- Mollie (betalingsverwerker)
- Google (Gmail, Google Agenda en Google Drive)
- Teamleader (CRM systeem)
- IXL (webhosting)

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:

Angsthelden draagt zorg voor de toegangsbeveiliging van de gebruikte apparaten en systemen:

- De telefoon is beschermd met een pincode en ontgrendelingscode;
- De computer is beschermd met een toegangscode;
- Gmail is beschermd met een gebruikersnaam en wachtwoord;
- Google Agenda is beschermd met een gebruikersnaam en wachtwoord;
- Google Drive is beschermd met een gebruikersnaam en wachtwoord;
- Teamleader is beschermd met een gebruikersnaam en wachtwoord.

Daarnaast maakt Angsthelden gebruik van een afgeschermd WiFi-netwerk met WPA2 beveiligd wachtwoord.

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:

-Exact Online (software financiën) Beschikt over een assurance verklaring (ISAE 3402 type 2). Jaarlijks wordt de veiligheid van Exact Online geauditeerd.

-Mollie (betalingsverwerker) staat onder toezicht van specialisten op het gebied van databaseveiliging. Daarnaast voldoet Mollie aan alle richtlijnen voor de veiligheid van internetbetalingen, opgesteld door de Europese Bankautoriteit. Tevens staan zij onder permanent toezicht van de Nederlandsche bank.

-Gmail (mail verkeer) Waar mogelijk beschermt Gmail informatie door e-mails automatisch te versleutelen. Ze worden dan tijdens de bezorging omgezet in een code. Deze beveiligingstool heet Transport Layer Security (TLS) en voorkomt dat anderen je e-mails kunnen lezen.

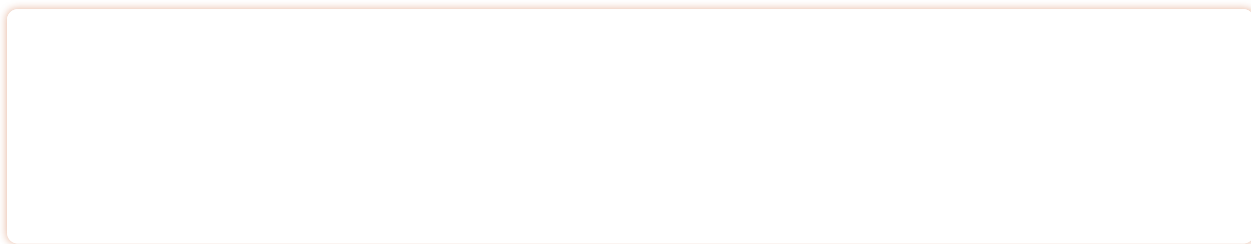
-Google Agenda (agenda voor ingeplande trainingen) alle data in de agenda is versleuteld en daardoor enkel toegankelijk voor jou en personen met toegang tot Google haar goed beveiligde data servers.

-Google Drive (online opslag) Google scant automatisch alle bestanden die gedeeld zijn op phishing of malware. Als Google vermoedt dat een bestand spam is, wordt het geblokkeerd of als spam gemarkeerd. Daarnaast maakt Google gebruik van reCAPTCHA om gebruikers te beschermen tegen bedrieglijke en misbruik makende activiteiten in Google Drive.

-Teamleader (CRM-systeem) is ISO 27001, SOC 1 en SOC2/SSAE 16/ISAE 3402 (voorheen SAS 70 Type II), PCI Level 1, C5 Operational Security, ENS High en IT-Grundschutz gecertificeerd. Jaarlijks wordt veiligheid van Teamleader geauditeerd.

-IXL (webhosting) is ISO 27001, NEN7510 en ISO9001 gecertificeerd.

Onderdeel van deze audits is software wat up-to-date is. Dit gebeurt automatisch op de achtergrond, waardoor Angsthelden alle externe software up-to-date heeft. Daarnaast zorgen medewerkers voor up-to-date software op computers, dit gebeurt door de automatische updates vanuit de computersystemen.



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.
- ☐ Wij als organisatie verklaren dat wij ook persoonsgegevens overdragen aan of opslaan bij partijen die gevestigd zijn buiten de EU. Wij hebben hiervoor de correcte maatregelen en overeenkomsten afgesloten. Onze situatie hebben wij hieronder beschreven.

Beschrijf hieronder kort uw situatie:

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:

De gebruikte software zorgt voor automatische online back-ups van de persoonsgegevens.

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 uw situatie:

Enkel het management bestaande uit: Niels Polak, Wouter Ruikes en Giel Dietzenbacher hebben toegang tot de persoonsgegevens uit Exact Online en Mollie. Daarnaast heeft het management en het secretariaat toegang tot persoonsgegevens uit de (agenda)systemen van Google Agenda, Gmail, Google Drive en Teamleader. Enkel personen die in deze persoonsgegevens moeten kunnen zijn daartoe geautoriseerd.

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

Wij als organisatie hebben 7 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 441 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:

Angsthelden bewaart persoonsgegevens in de eerder genoemde systemen. Indien een persoon wenst dat zijn/haar persoonsgegevens verwijderd worden, geeft Angsthelden hier gehoor aan. De gegevens zullen worden vernietigd door het verwijderen van alle gegevens uit alle systemen en eventueel via de papierversnipperaar voor papieren documenten.

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:

Uw situatie:

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:

Uw situatie:

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:

Alle trainers bewaren papieren aantekeningen thuis in een afgesloten kast.

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:

Een data wordt gemeld bij mede-eigenaar Niels Polak. Binnen 72 uur na het vaststellen van het datalek zal contact gezocht worden met de Autoriteit Persoonsgegevens voor eventuele verdere stappen.

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:

Vast agendapunt op teamoverleggen. Indien er geen teamoverleg is op korte termijn, dan vindt overleg plaats via mail of telefoon. Afhankelijk van de urgentie.

Privacy bescherming is een vast agendapunt op teamoverleggen van Angsthelden. Dit is het moment waarop het management eventuele nieuwe ontwikkelingen met de behandelaren bespreekt. Tegelijkertijd delen trainers eventueel processen/inzichten die zij opgedaan hebben bij andere soortgelijke organisaties.

16.3 Afronding

Naam organisatie:

Angsthelden

Plaats:

Nijmegen

Datum:

31-8-2023

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.