

AVG verklaring

Drukkerij Riezebos BV

Uitgegeven op 18-3-2025



Geldig tot 18-6-2025

Stichting AVG voor Verenigingen
Doctor Kuiperstraat 10
2514 BB Den Haag
www.stichting-avg.nl

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!

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

Drukkerij Riezebos BV 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 Drukkerij Riezebos BV 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 Drukkerij Riezebos BV zijn te vinden op de volgende pagina(s) van deze verklaring.

Aldus opgemaakt te Den Haag,

d.d. 18-3-2025,

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

Van relaties (klanten) gegevens tbv zakelijke dienstverlening: klant/debiteurnummer, kvk nummer, iban, bic, btw-nummer, profiel/type klant (categorie), prijsafspraken, orderinformatie en betaalhistorie, facetime-, skype en whatsapp gegevens (en gekoppelde gegevens van relaties, waaronder eventueel foto - dit niet op grote schaal). Daarnaast variabele persoonsgegevens verstrekt door klanten in bestanden t.b.v. realisatie / expeditie van drukwerk. Marketing gegevens in cloudoplossing Copernica. Gegevens over computer- en applicatiegebruik van eigen medewerkers.

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

De meeste bijzondere persoonsgegevens (salaris, paspoort kopie, BSN) zijn aanwezig vanwege de personeelsadministratie, en wettelijk noodzakelijk (grondslag).

Als Verantwoordelijke kan Riezebos op kleine schaal of voor prive-gebruik van medewerkers kunnen foto's met personen en/of locatie opslaan op netwerkschijven. Overige foto's zullen alleen aanwezig zijn in verband met opdracht door een klant, waardoor de klant verwerkersverantwoordelijke is.

Naast per wet officiële bijzondere gegevens, noemen we hier (mogelijke) gevoelige gegevens, waar Drukkerij Riezebos extra aandacht heeft voor de resultaten voor het (mogelijk algemeen geldend) minimale beveiligingsniveau.

Daarnaast variabele persoonsgegevens verstrekt door klanten in bestanden t.b.v. realisatie / expeditie van drukwerk.

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

NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens, gegevens rondom de verstrekte opdracht. Indien er bij uitvoering van een opdracht een klacht wordt ontvangen, zijn deze gegevens ook geregistreerd. Bewaartermijn van gegevens is oneindig, tot verzoek van betrokkene tot verwijdering of periodieke opschoonactie van ons bedrijf.

Voor de realisatie van de opdracht kunnen variabele sets persoonsgegevens door de klant aangeleverd worden (variabel drukken, bezorging). Deze gegevens worden binnen 2 weken na afronding en facturatie van de opdracht verwijderd (zie ook verder in dit tool).

M.b.t. leveranciers zijn - op zakelijk niveau enigszins gevoelig - prijsafspraken aanwezig. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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

De ontvanger van de nieuwsbrief kan zelf kiezen aanvullende NAW of profielgegevens te verstrekken om meer gerichte informatie te krijgen. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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

Bewaartermijn is oneindig, tot verzoek verwijdering. NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens, gegevens rondom de verstrekte opdracht. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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

Bij uitzondering incidenteel aanwezig, door middel van e-mail adres van prospects en enkele opdrachten. Deze worden niet toegepast met doeleinden het politieke aspect te benadrukken - dit is een toevallig kenmerk van de primaire activiteit van de organisatie, het maken en leveren van communicatiematerialen. Bewaartermijn is oneindig, tot verzoek verwijdering.

NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens, gegevens rondom de verstrekte opdracht. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verdwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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

BSN (in kopie ID)
 Bewaartermijn is tenminste 7 jaar (belastingdienst).
 NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verdwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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

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

NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens, gegevens rondom de verstrekte opdracht. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

- 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.

NAWTE - wij gebruiken een CRM systeem (Drumis) waarin enkele aanvullende gegevens zijn opgeslagen, zoals social media adressen/contactgegevens, gegevens rondom de verstrekte opdracht. Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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:

ICT BEHEER

Doel: technisch beheer van ICT systemen in de organisatie

Persoonsgegevens: aan gebruiker gekoppelde informatie (toegang tot domein en applicatie, ip-adres, surfgedrag, intern gebruik, incidenten/storingen, enz.)

Grondslag: Vitaal belang (medewerkers) en uitvoering overeenkomst / aantoonbaar akkoord (bedienen relaties die gebruik maken van het digitale contactformulier op de website en het marketingsysteem Copernica).

Verwerkingen: automatische registratie t.b.v. ICT systeembeheer (medewerkers) en ontzorgen bezoekers website (communicatie afhandelen)

Bewaartermijn: automatische logging met ingestelde duur van loggen (verwachting: een maand) voor het eigen ICT systeem (toegang tot bezochte websites wordt niet gelogd) en tot verzoek verwijdering (door klanten) uit systemen van Riezebos (Copernica, Drumis)

CAMERATOEZICHT

Doel: beveiliging van het pand en bedrijfsmiddelen

Persoonsgegevens: Camerabeelden van personen

Grondslag: Vitaal belang + informering omgeving door middel van borden/stickers cameratoezicht

Verwerkingen: Direct toezicht (geen vastlegging) en bij incidenten/voorvallen voor evt. melding politie

Verwerking door wie: Directie

Bewaartermijn: 14 dagen (cyclisch overschrijven)

PRODUCEREN VAN DRUKWERK VOOR KLANTEN

Persoonsgegevens: variabel (aangeleverd door klant)

Grondslag: noodzakelijk voor uitvoering van een contract

Verwerkingen: digitale bestandsverwerking, pre-press, drukwerk, nabewerken, logistiek, facturatie

Verwerking door wie: verkoop, administratie, productie

Bewaartermijn: gegevens t.b.v. de orderstroombeheersing: oneindig, tot verzoek verwijdering (maar met behoud van wettelijk noodzakelijke geregistreerde gegevens (belastingdienst)). gegevens voor inhoudelijke productie: 14 dagen (t.b.v. ondersteuning klant een korte periode na uitvoering van de opdracht).

SOLLICITANTEN (op dit moment alleen open sollicitaties)

Doel: geen (open sollicitaties worden wel eens ontvangen, maar na respons dat er geen vacature is, worden deze gegevens verwijderd).

Met betrekking tot alle voorgaande geldt het volgende: Wij maken van deze gegevens een backup. In deze backup worden deze gegevens (niet live) oneindig bewaard. Indien er een verwijderverzoek is, duurt het maximaal een maand na de doorgevoerde verwijderactie totdat de gegevens ook uit de backup verwijderd zijn.

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:

De website www.drukkerijriezebos.nl heeft deze privacy disclaimer (per 24 mei 2018).

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 als organisatie doen dit per 24 mei 2018.

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:

Vanaf 24 mei 2018 werken wij met verwerkersovereenkomsten met:
ICT dienstverlening (systeembeheerder en onze aanbieder van de nieuwsbrief voor marketingdoeleinden)
Productiepartners (als wij een opdracht niet helemaal zelf produceren)
Boekhouding
Logistieke dienstverlening
Arboarts en arbodienst

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:

Gebruikersnaam en wachtwoord zijn ingericht op de werkstations en de email toepassingen, maar moeten meer afgedwongen worden, door middel van:

- Inloggen op PC's (en productiemachines, indien relevant/mogelijk) (wachtwoord onthouden uitzetten op machines die VPN gebruiken)
 - Wachtwoordbeveiliging bij computers/smartphones die toegang hebben tot de mailapplicaties van Drukkerij Riezebos. (voor webmail ook het onthouden van wachtwoorden in de browser uitzetten).
- Met betrekking tot fysieke dossiers: achter slot en grendel, onder beheer directeur (met name personeelsdossier).

Tijdens de inventarisatie bleken er geen digitale personeelsgegevens te zijn. Om dit in de toekomst (en andere gegevens) op te kunnen slaan, wordt een netwerkmap met beperkte toegangsrechten aangepast tot een MT map.

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:

Terminals en individuele werkstations hebben automatisch uitgevoerde patches. Servers worden door ICT beheerder handmatig, maar tenminste eens per maand geüpdatet. Software-updates die door de leveranciers als 'kritiek' aangemerkt worden, worden pro-actief door ICT beheerder zsm doorgevoerd.

M.b.t. antivirus: beide servers hebben antivirusscanner, die inkomende mail en netwerkmappen worden gescand. Er is geen endpoint scanning, waardoor er risico is op infectie via usb-stick of phishing/malware mail.

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:

Alles binnen EER, waar niet dan vallend onder Privacy Shield. (controle iCloud wordt nog uitgevoerd).

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:

Incremental backups van files (klantbestanden, bestanden in netwerkmappen en database files (waaronder Drumis) en mailstructuur worden uitgevoerd met een variabele retentietijd, welke maximaal 1 maand is op basis van de resterende opslagruimte. Incremental backup wordt dagelijks gedaan en alleen gedurende de tijd van de backup gekoppeld aan het systeem, met gebruik van 2 roterende schijven (waarbij de schijf in start is voorzien van de onderliggende full backup). Restores worden uitgevoerd op bestandsniveau. De cloudoplossing 'Copernica' maakt gebruik van live mirror databases en dagelijkse snapshot.

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:

Onze organisatie is dusdanig klein dat veel informatie gedeeld wordt (moet worden om aan contractuele verplichtingen te kunnen voldoen) Uitzondering hierop zijn de eigen personeelsgegevens.

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

Wij als organisatie hebben _____ 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 _____ 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:

Backup- en verwijderprotocol:

- (backups nader te omschrijven, per 24 mei 2018 geregeld)
- van alle personen die verzocht hebben dat hun gegevens verwijderd moeten worden, wordt een dossier bijgehouden zolang er kans is dat deze gegevens nog in de backup aanwezig zijn en dus via een restore weer actief kunnen worden voor de organisatie. Daarbij is het ook van belang dat het verwijderen van gegevens niet in een kopie-bestand gebeurt (waardoor het origineel nog gebackupid zou zijn).

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:

Toestemming wordt gevraagd door medewerkers, gegeven door de betrokkenen zoals omschreven bij onze bepaling van doelbinding bij klantgegevens, gevraagd en vastgelegd via (contact)formulier website (per 24-05-2018) en onze privacy policy is zichtbaar op onze website en via verwijzing in onze offertes / orderbevestigingen (overweeg: in de handtekening van elke e-mail). Historische gebruikers die deze toestemming in het verleden niet aantoonbaar hebben gegeven worden geïnformeerd dat ze de kans hebben zichzelf alsnog uit het CRM van Riezebos te verwijderen (ook als ze al geen e-mails meer zouden krijgen).

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:

Wij verzorgen geboortekaartjes op basis van directe aanvraag van familie. Hiervoor hebben wij geen handtekening op papier. Wij hebben via onze adviseur de vraag aan de autoriteit persoonsgegevens gesteld of ook in dit geval een schriftelijke handtekening op papier noodzakelijk is.

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:

Eigen persoonsgegevens (fysieke dossiers van personeel en prints van CRM-informatie) zijn respectievelijk opgeslagen in een afsluitbare kast, of alleen binnen het bedrijf aanwezig (dan niet bijzonder gevoelig) - het bedrijf heeft uiteraard goede fysieke beveiliging, waaronder alarm en cameratoezicht.

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:

Beoogd is voor de 24e mei 2018 de benodigde informatie aan de medewerkers te verstrekken. Men is ervan op de hoogte dat elk (potentieel) datalek intern gemeld wordt aan Gerrit Riezebos, die evalueert wat de potentiële impact is de betrokkene (en klant, indien aanwezig) en op basis van de richtlijnen voor melding van een datalek, zoals gepubliceerd door de Autoriteit Persoonsgegevens, melding doet wanneer nodig.

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:

Voor 24 mei zijn bovengenoemde punten beoogd om uit te voeren.

16.3 Afronding

Naam organisatie:

Drukkerij Riezebos BV

Plaats:

De Lier

Datum:

15-02-2024

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.