

Privacybeleid KDV Pindakaas



Inhoud

1. AVG wetgeving	3
2. Privacy rechten werknemers.....	3
3. Beveiligingsbeleid.....	4
4. Procedure meldplicht datalekken	7
5. Incidentenlijst 2019.....	8
6. Toestemming gegevens sollicitanten	9
7. Toestemming publicatie	9
8. Evaluatie	10
9. Bijlagen	11
Bijlage 1: Verwerking persoonsgegevens volgens AVG wetgeving.....	12
Bijlage 2: Inventarisatie gegevensstromen	13
Bijlage 3: Stappenplan meldplicht Datalekken.....	14

1. AVG wetgeving

Per 25 mei 2018 is de wet AVG (Algemene Verordening Gegevensbescherming) van kracht. In opvolging van deze wet is dit privacy beleid opgesteld. In bijlage 1 is te vinden aan welke beginselen het verwerken van gegevens moet voldoen en hoe wij daar aan voldoen.

De AVG stelt dat je bij het verwerken van gegevens verschillende rollen hebt.

1. De verwerkingsverantwoordelijke: als je zelf het doel en de middelen bepaalt voor de verwerking met je verantwoordelijke.

Bijvoorbeeld voor de personeelsgegevens van je eigen personeelsbestand.

2. De verwerker: als je de persoonsgegevens uitsluitend ten behoeve van de dienstverlening aan een opdrachtgever verwerkt, ben je verwerker.

Bijvoorbeeld: onze IT-leverancier die onze email beheerd. Hij bepaald niet het doel en de middelen van de binnenkomende mail, hij verwerkt alleen de gegevens voor ons, zonder zeggenschap te hebben over de verwerking er van.

Pindakaas heeft inzicht verkregen in de gegevensstromen die plaatsvinden en welke rol wij daar in hebben. Hierbij hebben wij antwoord gegeven op de volgende vragen:

- Welke administraties zijn er?
- Welke registraties zijn er?
- Zijn er nog andere systemen/plaatsen waar zich gegevens bevinden?

In bijlage 2 kun je het overzicht vinden van deze inventarisatie.

Op basis van deze registratie hebben wij een verwerkingsregister opgesteld. In dit register staat alle gegevensverwerking die plaatsvindt bij Pindakaas, de betrokkenen, de doelen en grondslag van de verwerking. Daarnaast wordt omschreven wie toegang heeft tot de gegevens, of de gegevens worden verstrekt aan derden en wat het bewaartermijn is. Tot slot wordt aangegeven hoe we betrokkenen informeren over de verwerking en hoe we op juistheid controleren. In dit verwerkingsregister is ook ons DPIA verwerkt: wij beschrijven risico's en beveiligingsmaatregelen. Het verwerkingsregister is een los bestand naast dit privacy beleid.

Als bijlage van dit document zijn ook de privacy verklaringen opgenomen. Hierin staat vermeld welke gegevens wij van klanten en medewerkers verwerken en met welke doelen. Dit is een openbaar document dat op onze website staat

2. Privacy rechten werknemers

Alle betrokkenen van de verwerking van persoonsgegevens hebben volgens de AVG een aantal rechten. Hieronder lichten wij deze kort toe.

Recht op informatie

Alle werknemers hebben het recht om (tijdig) informatie te krijgen over de verwerking van zijn persoonsgegevens, het doel waarvoor ze gebruikt worden en waar de werknemer naartoe kan als hij een klacht heeft.

Recht op inzage

Een werknemer heeft het recht om zijn personeelsdossier in te zien en hij heeft het recht om er een

kopie van op te vragen. Een werkgever dient dit te verstrekken.

Recht op rectificatie

Een werknemer kan van een werkgever verwachten dat onjuiste gegevens worden aangepast of worden aangevuld.

Recht van bezwaar

Een werknemer heeft te allen tijde recht om bezwaar te maken tegen de verwerking van bepaalde persoonsgegevens. (artikel 21 AVG)

Het recht op vergetelheid

Een werkgever is verplicht om persoonsgegevens van een werknemer zonder onredelijke vertraging (1 maand) te verwijderen als de verwerking niet langer nodig is voor het afgesproken doel, of als de werknemer zijn instemming intrekt.

Recht op beperking van verwerking

Dit houdt in dat persoonsgegevens niet verwerkt of gewijzigd mogen worden. Dit geldt voor specifieke situaties (artikel 18 AVG)

Bijvoorbeeld: de werkgever heeft de gegevens niet meer nodig voor de doeleinden genoemd in de privacyverklaring, maar de werknemer heeft de gegevens nog nodig voor een andere instelling (UWV) of onderbouwing van bijvoorbeeld een rechtszaak.

Recht op overdraagbaarheid (dataportabiliteit)

Een werknemer heeft het recht zijn data mee te nemen en dus op een gemakkelijke manier over te kunnen dragen aan een derden.

Bijvoorbeeld: als een werknemer een andere baan heeft, kan de werknemer vragen zijn of haar persoonsgegevens vanuit Pindakaas mee te nemen naar de andere werkgever. Dit kan zowel digitaal als op papier.

Het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming

Dit recht houdt in dat een sollicitatie bijvoorbeeld niet zomaar verwerkt kan worden via internet, zonder menselijke tussenkomst.

Bijvoorbeeld: sollicitaties mogen niet automatisch worden beantwoord door een computersysteem.

Ouders en werknemers van Pindakaas kunnen te allen tijde het privacybeleid en de privacyverklaring raadplegen op de website. Ons verwerkingsregister is tevens in te zien door werknemers op onze online database.

3. Beveiligingsbeleid

Voor sommige ondernemingen is het verplicht om een (D)PIA uit te voeren: een Data protection impact assessment (gegevensbeschermingseffectbeoordeling) uit te voeren. Dit is een risicoanalyse voor de bestaande verwerkingen. Wij hebben onze risico-analyse verwerkt in ons verwerkingsregister.

Om de beveiliging van persoonsgegevens goed te waarborgen, hebben wij, op basis van de risico-analyse, een beveiligingsbeleid opgesteld. Hierin staan technische en organisatorische maatregelen

waarmee wij de persoonsgegevens van onze klanten en werknemers beveiligen. Deze staan ook vermeld in het verwerkingsregister en werken we hier uitgebreider uit.

Technische maatregelen: toegang tot gegevens

- Wachtwoord op desktop

Wij werken met 3 computers op kantoor. Op 2 computers zit een wachtwoord. Op deze computer worden persoonsgegevens bewaard en staat de software met persoonsgegevens. Op de andere desktop staan geen persoonsgegevens bewaard. Onbevoegden kunnen de beveiligde computer niet opstarten zonder een bevoegd persoon er bij. Alleen de directeur en beleidsmedewerker weten het wachtwoord.

- Wachtwoord op kenniscentrum

Alleen medewerkers en stagiaires die werkzaam zijn hebben toegang tot ons kenniscentrum. Zodra een dienstverband eindigt of de stage er op zit, wordt de toegang tot het kenniscentrum geblokkeerd.

- Wachtwoord op specifieke mappen binnen ons kenniscentrum zoals: kinddossier

Om de toegang nog meer te specificeren hebben wij een extra beveiliging op bepaalde mappen gezet die maar voor 1 of 2 mensen toegankelijk zijn. Alleen de directeur, beleidsmedewerker en VVE-coördinator kunnen bij deze map.

- Firewall voor onze online omgeving

Wij maken gebruik van een remote management systeem waar onder andere de zakelijke antivirus applicatie Bitdefender in verwerkt zit. Bitdefender voert 11 miljard beveiligingscontroles per dag uit en detecteert zelfs de nieuwste dreigingen al binnen 3 seconden na hun verschijnen, waar ook ter wereld, voor efficiënte anticipatie en eliminatie van alle dreigingen.

Daarnaast zit er een website screening applicatie in welke websites screent en mogelijk blokkeert indien zaken niet in orde (lijken te) zijn en/of een bepaalde categorie hebben. Dit is van de leverancier BrightCloud.

- Wachtwoord op software waarin gegevens worden verwerkt.

Op onze softwareprogramma's "Konnnect, The Nanny, Zasalari, OVM en onze mailaccounts zit een beveiliging door middel van een wachtwoord. Alleen bevoegden weten dit wachtwoord. De beveiliging van deze softwarebedrijven zelf, is beschreven in de verwerkerovereenkomst.

Email versleuteld verzenden

- In een aantal gevallen verzenden wij persoonlijke informatie per mail. Dit gebeurt in contact met: het consultatiebureau, de GGD, de gemeente en de basisscholen. Deze bijlagen in deze emails verzenden bij versleuteld met een wachtwoord. Dit wachtwoord geven we vervolgens telefonisch door aan de ontvanger. Zo weten wij dat alleen de ontvanger de email kan openen. Hun eigen privacy beleid is daarna leidend in het verwerken van de e-mail.

Organisatorische maatregelen

- Personenregister Kinderopvang

Al onze medewerkers hebben een VOG aangevraagd en zijn ingeschreven bij het Personenregister Kinderopvang. Dit betekent dat zij onder continu screening staan op onder andere het omgaan met gevoelige en vertrouwelijke informatie.

- Clean desk policy

We werken met flex-plekken. Zodra je werkdag er op zit ruim je je bureau op en berg je informatie met persoonsgegevens op.

- Afgesloten dossierkast

Op kantoor hebben wij een dossierkast die op slot kan. Hier staan onze (niet openbare) papieren databases in zoals de personeelsgegevens, sollicitaties, gegevens van stagiaires en archieven. De directeur, beleidsmedewerker en dagmanager BSO hebben toegang tot deze kast.

- Dataminimalisatie en opslagbeperking

Door ons (beveiligde) kenniscentrum hebben wij zo weinig mogelijk papieren gegevens op kantoor. Oude gegevens worden direct verwijderd als er een aanpassing is geweest. Zo blijven persoonsgegevens niet slingeren.

- Veilige postverwerking

Onze uitgaande post wordt op kantoor in een gesloten envelop klaargelegd en door medewerkers naar de brievenbus gebracht. Inkomende post wordt gesloten in het postvak van de directeur van Pindakaas gelegd.

- Papierversnipperaar

Wij hebben een papierversnipperaar op kantoor waar we gegevens mee vernietigen die de bewaartermijn hebben bereikt of die niet meer nodig zijn voor het bereiken van het doel.

4. Procedure meldplicht datalekken

Als er binnen een bedrijf een grote datalek is, dan is de organisatie verplicht om dit te melden bij het AP (Autoriteit Persoonsgegevens) en de betrokkenen moeten worden geïnformeerd. Binnen de AVG wet is bepaald dat organisaties een incidentenregister moeten bijhouden. Hierin worden incidenten vermeld die te maken hebben met (persoons)gegevens, ook diegene die niet gemeld hoeven te worden bij AP.

Bij een datalek kun je bijvoorbeeld denken aan:

- *een hack op ons emailsysteem of website*

Bij een incident kun je denken aan:

- *een email die naar de verkeerde ontvanger wordt verzonden, maar op afstand kan worden gewist.*

- *een brief die naar de verkeerde ontvanger is gestuurd, maar ongeopend retour wordt verzonden*

In hoofdstuk 5 is de incidentenlijst te vinden.

In bijlage 3 is een stappenplan te vinden waarin we stapsgewijs laten zien hoe we beoordelen of een gebeurtenis een incident of datalek is en wanneer we een melding moeten doen bij het AP/ betrokkenen moeten informeren.

6. Toestemming gegevens sollicitanten

Wij vragen sollicitanten toestemming om gegevens 1 jaar te bewaren in onze (papieren) database.

Dit doen wij door een mail te sturen zodra de sollicitant per mail een sollicitatiebrief en/of CV heeft toegestuurd.

Wij printen de sollicitatiebrief, CV en toestemming uit en doen deze in onze papieren database, in een afgesloten kast.

Volgens de AVG wetgeving moet het vragen van toestemming Vrij, specifiek, geïnformeerd en ondubbelzinnig zijn.

Vrij: de betrokkene heeft een keuze om toestemming te geven of niet.

Specifiek: de verwerking is voldoende concreet omschreven.

Geïnformeerd: wat gebeurd er met de verwerking en wie kan de gegevens inzien.

Ondubbelzinnig: geen twijfel over het feit of de betrokkene zijn toestemming heeft gegeven.

Op basis van bovenstaande eisen versturen wij de volgende tekst naar sollicitanten:

Beste heer/mevrouw,

Bedankt voor uw interesse en sollicitatie bij KDV/BSO Pindakaas. Op dit moment hebben wij geen openstaande vacature. Wellicht hebben wij in de toekomst wel een vacature waar uw profiel bij past.

Wij willen u vragen of wij uw sollicitatiebrief, NAW gegevens en CV mogen bewaren in onze papieren database (in een afgesloten archiefkast), voor de duur van 1 jaar. Wij gebruiken uw gegevens alleen als wij een geschikte vacature voor u hebben. Na het verstrijken van het termijn van 1 jaar vernietigen wij uw gegevens. Uw gegevens worden niet verstrekt aan derden. Alleen de directeur en pedagogisch beleidsmedewerker van Pindakaas kunnen uw gegevens inzien.

Ik ontvang graag een antwoord op deze mail waarin u aangeeft of u wel of niet akkoord gaat met bovenstaande.

Met vriendelijke groet,

KDV Pindakaas

7. Toestemming publicatie

Wij gebruiken foto's die dagelijks in de Konnect app worden gemaakt ook voor publicaties op Facebook, onze website, onze folders, mappen en posters en voor de nieuwsbrief. Wij vragen ouders schriftelijk toestemming via ons inschrijfformulier. Ouders kunnen te allen tijde hun toestemming intrekken. Hierover worden zij geïnformeerd in onze privacyverklaring.

Op basis van de eisen voor het vragen van toestemming staat de volgende tekst op ons inschrijfformulier:

*Ik geef toestemming voor het openbaar plaatsen van foto's/filmpjes van mijn kind op:
de facebookpagina van pindakaas ja/nee * de website van pindakaas ja/nee * de folders en mappen van pindakaas ja/nee * de posters van pindakaas ja/nee * de nieuwsbrief van pindakaas ja/nee*

8. Evaluatie

2018 (evaluatie op 15-4-2019)

In 2018 is het plan in mei van start gegaan. Wij evalueren dit plan ieder jaar in April.

In 2018 is dit plan als prettig ervaren. De invoering van de AVG heeft bewustzijn gecreëerd over hoe we met persoonsgegevens omgaan. De maatregelen die nodig waren om dit zo optimaal te laten verlopen zijn ingevoerd en lopen goed. Er zijn dit jaar geen datalekken geweest. We hebben inmiddels 3 vaste computers, dus dat is in het plan aangepast. Verder is het plan ongewijzigd vastgesteld.

2019 (evaluatie op 15-4-2020)

9. Bijlagen

- 1. Verwerking persoonsgegevens volgens AVG wetgeving**
- 2. Inventarisatie verwerking gegevens**
- 3. Stappenplan meldplicht datalekken**

Bijlage 1: Verwerking persoonsgegevens volgens AVG wetgeving

Gegevensverwerking moet voldoen aan de volgende beginselen:

Persoonsgegevens moeten:

1. Rechtmatig, behoorlijk en transparant worden verwerkt.

Acties:

Rechtmatig: grondslag en doel staat in ons verwerkingsregister

Behoorlijk: de gegevens staan in een afgesloten kast of gesloten online database

Transparant: medewerkers en klanten mogen te allen tijde hun persoonsgegevens in zien (dit staat in het privacybeleid).

2. Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd

Acties:

- doelen voor verwerking zijn opgenomen in het verwerkingsregister

3. Toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking”);

Acties:

- welke gegevens worden verwerkt is opgenomen in het verwerkingsregister met bijbehorend doel.

4. Juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren

Acties:

- Hoe wordt omgegaan met juistheid en wissen/rectificeren van gegevens is opgenomen in het verwerkingsregister.

5. Worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig.

Acties:

- Het bewaartermijn is opgenomen in het verwerkingsregister

6. Door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).

Acties:

- De beveiliging van de persoonsgegevens is opgenomen in het verwerkingsregister

Bijlage 2: Inventarisatie gegevensstromen

Hieronder staat een eerste inventarisatie van de gegevensstromen binnen Pindakaas. In het verwerkingsregister zijn deze stromen verder uitgewerkt.

Welke administraties (veranderlijk, wordt bijgehouden) zijn er	Omgeving	Worden er persoonsgegevens verwerkt?	Rol van Pindakaas
Kind administratie Konnect (app)	Digitaal	Ja	Verwerkingsverantwoordelijke
Kind administratie Saamn	Digitaal	Ja	Verwerkingsverantwoordelijke
Personeelsadministratie	Papier	Ja	Verwerkingsverantwoordelijke
Personeelsapp	Digitaal	Ja	Verwerkingsverantwoordelijke
Salarisadministratie (Zasalaris)	Online	Ja	Verwerkingsverantwoordelijke
OVM (Ontwikkeling volgmodel)	Desktop app	Ja	Verwerkingsverantwoordelijke
Overstap	Papier	Ja	Verwerkingsverantwoordelijke
Consultatiebureau	Digitaal en papier	Ja	Verwerkingsverantwoordelijke
Accountantskantoor	Digitaal	Ja	Verwerkingsverantwoordelijke

Welke registraties (vastgezet) zijn er	Omgeving	Worden er persoonsgegevens verwerkt?	Rol
E-mailverkeer (Dacon)	Online	Ja	Verwerkingsverantwoordelijke
Inschrijfformulieren	Papier	Ja	Verwerkingsverantwoordelijke
Contracten	Papier	Ja	Verwerkingsverantwoordelijke
Telefoonregistraties	Papier	Ja	Verwerkingsverantwoordelijke
Sollicitaties	Papier	Ja	Verwerkingsverantwoordelijke
Facebook	Online	Ja	Verwerkingsverantwoordelijke
Website	Online	Ja	Verwerkingsverantwoordelijke
PR materiaal (mappen/folders)	Papier	Ja	Verwerkingsverantwoordelijke
Kind dossiers	Online	Ja	Verwerkingsverantwoordelijke

Het Kenniscentrum is geen gegevensstroom omdat hier geen persoonsgegevens worden verwerkt.

Bedrijven waar wij mee samenwerken, die gegevens verwerken voor de dienstverlening naar ons, worden in de AVG wet “verwerkers” genoemd. Met deze verwerkers moet Pindakaas (als “verwerkingsverantwoordelijke”) mee worden gemaakt d.m.v. een verwerkersovereenkomst. In een verwerkersovereenkomst staan (samenvattend) de volgende punten beschreven:

- Welke gegevens de verwerker verwerkt en met welk doel
- Hoe de verwerker zijn gegevens beveiligd
- Afspraken over datalekken

Deze verwerkersovereenkomsten worden door beide partijen ondertekend. De partijen waar een verwerkersovereenkomst mee is afgesloten:

- Konnect
- Saamn
- Dacon
- OVM
- Zasalaris / Tactiplan

- Arboned
- Accountantskantoor

Bijlage 3: Stappenplan meldplicht Datalekken

Iedereen heeft recht op bescherming van zijn of haar persoonsgegevens. Hieronder een kort schema waarin wij laten zien hoe wij bepalen of iets een datalek is of niet. (Bron: Autoriteit Persoonsgegevens)

De meldplicht is voor gegevens die geheel of gedeeltelijk geautomatiseerd worden verwerkt of persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om in een bestand te worden opgenomen.

